



(51) Internationale Patentklassifikation ⁶ : G07F 7/10, 7/08		A1	(11) Internationale Veröffentlichungsnummer: WO 99/00773
			(43) Internationales Veröffentlichungsdatum: 7. Januar 1999 (07.01.99)
(21) Internationales Aktenzeichen: PCT/CH98/00282		(81) Bestimmungsstaaten: AL, AM, AT, AT (Gebrauchsmuster), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Gebrauchsmuster), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).	
(22) Internationales Anmeldedatum: 29. Juni 1998 (29.06.98)			
(30) Prioritätsdaten: 1564/97 27. Juni 1997 (27.06.97) CH PCT/CH98/00086 5. März 1998 (05.03.98) WO (34) Länder für die die regionale oder internationale Anmeldung eingereicht worden ist: CH usw.			
(71) Anmelder (für alle Bestimmungsstaaten ausser US): SWISS-COM AG [CH/CH]; Viktoriastrasse 21, CH-3050 Bern (CH).			
(72) Erfinder; und		Veröffentlicht	
(75) Erfinder/Anmelder (nur für US): RITTER, Rudolf [CH/CH]; Rossweidweg 8, CH-3052 Zollikofen (CH). BOUQUET, Hanspeter [CH/CH]; Kappelenring 49A, CH-3032 Hinterkappelen (CH). HEUTSCHI, Walter [CH/CH]; Jungfrauweg 8, CH-3303 Jegensdorf (CH).		Mit internationalem Recherchenbericht.	
(74) Anwalt: BOVARD AG; Optingenstrasse 16, CH-3000 Bern 25 (CH).			

(54) Title: TRANSACTION METHOD CARRIED OUT WITH A MOBILE APPARATUS

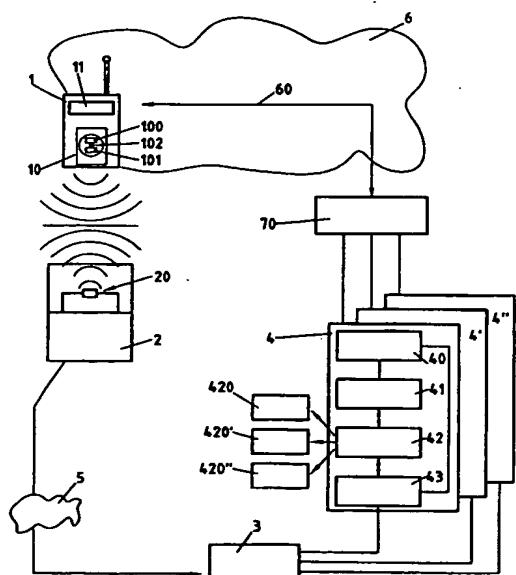
(54) Bezeichnung: TRANSAKTIONSVERFAHREN MIT EINEM MOBILGERÄT

(57) Abstract

The invention relates to a method for carrying out financial transactions between a client equipped with a mobile telephone and an electronic terminal (2), where said mobile telephone comprises a mobile apparatus (1) and a detachable identification module in which at least one client identification element and one electronic sum of money can be memorized. Said method comprises each of the following steps: reloading of the given sum of money by means of secured reloading documents via the mobile telephone network from a service centre (4), transmission of the client identification element to the terminal (2) via a contactless interface between the identification module (10) and the terminal (2), verification in said terminal that the client identified by means of the aforementioned transmitted client identification element is authorized to carry out a financial transaction, said verification being carried out with authorization data transmitted to the terminal (2) via a public connected telephone network (5), and transmission of a transaction amount to the terminal (2) via the contactless interface.

(57) Zusammenfassung

Finanztransaktionsverfahren zwischen einem mit einem Mobilfunktelefon ausgerüsteten Kunden und einem elektronischen Terminal (2), wobei das Mobilfunktelefon ein Mobilgerät (1) und ein wegznehmbares Identifizierungsmodul umfasst, in welchem mindestens eine Kundenidentifizierung und ein elektronischer Geldbetrag gespeichert werden können, wobei das Verfahren einen von jedem der folgenden Schritte umfasst: Nachladen des benannten Geldbetrages mit Hilfe von gesicherten Nachladebenlegen über das Mobilfunknetz aus einem Dienstzentrum (4); Übertragung der Kundenidentifizierung an das Terminal (2) über eine kontaktlose Schnittstelle zwischen dem Identifizierungsmodul (10) und dem Terminal (2); Prüfung im benannten Terminal der Erlaubnis des mit der benannten übertragenen Kundenidentifizierung identifizierten Kunden, eine Finanztransaktion durchzuführen, wobei diese Prüfung mit Erlaubnisdaten erfolgt, die an das Terminal (2) über ein öffentliches vermitteltes Fernsprechnetz (5) übertragen werden; Übertragung eines Transaktionsbetrages über die kontaktlose Schnittstelle an das Terminal (2).



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Transaktionsverfahren mit einem Mobilgerät

Die vorliegende Erfindung betrifft ein Verfahren und ein System zur Übermittlung von Aufträgen in einem Telekommunikationsnetz. Die Erfindung betrifft insbesondere, aber nicht ausschliesslich, die Übermittlung von Aufträgen 5 in einem Mobilfunknetz.

Gemäss dem bisherigen Stand der Technik werden Transaktionen zwischen einem Kunden (oder Client, C) und einem Terminal [Point-of-Transaktion (POT)], zum Beispiel einem Point-of-Sale (POS), oft mit einer elektronischen Zahlungskarte ausgeführt. Debit- und Kreditkarten werden zum 10 Beispiel an Kassen in Geschäften, bei Tankstellen, usw. verwendet. Die Karte umfasst meistens Speichermittel, zum Beispiel einen Magnetstreifen und/oder ein Chip, in welchem unter anderem die Identifizierung des Kunden gespeichert ist. Um eine Transaktion mit dem Besitzer oder Betreiber eines 15 Terminals zu tätigen, zum Beispiel um einen Artikel in einem Geschäft zu bezahlen, muss der Kunde seine Karte in einen geeigneten Kartenleser im Terminal einschieben. Der Terminal liest dann die Identifizierung des Kunden in der Karte, ermittelt und zeigt den zu bezahlenden Betrag an, prüft gegebenenfalls die Solvenz des Kunden und fordert vom Kunden, dass er die 20 Transaktion mit einer Bestätigungstaste auf dem Terminal bestätigt. Wenn der 25 Kunde solvent ist und seine Bestätigung eingegeben hat, werden die Kundenidentifizierung, der zu bezahlende Betrag und evtl. auch eine Terminal-Identifizierung an einen durch ein Telekommunikationsnetz mit dem Terminal verbundenen Finanzserver übermittelt, der von einem Finanzinstitut verwaltet wird. Entsprechend wird sofort oder später das Konto des Kunden bei diesem Finanzinstitut belastet.

Nachteilig in diesem Verfahren ist die Notwendigkeit, die Karte des Kunden in ein fremdes Gerät einschieben zu müssen. Die Kunden haben normalerweise ihre Karte nicht zur Hand, dafür zum Beispiel im Portemonnaie; eine sehr schnelle Transaktion ist also nicht möglich. Gelegentlich ist auch die 30 Öffnung zum Einführen der Karte in das Lesegerät des Terminals nicht leicht zugänglich; dies ist besonders dann der Fall, wenn der Terminal ein Ticketautomat für Parkhäuser oder ein Zahlungsautomat ist, der vom

Automobilisten ohne Aussteigen aus dem Wagen bedient werden soll.

Ausserdem können betrügerische Handlungen oder nicht berechtigte Lesungen von Speicherbereichen der Karte im Terminal durchgeführt werden.

Sogar wenn heutzutage gewisse Chipkarten einen Mikroprozessor
5 enthalten, sind diese Debit- und Kreditkarten im Wesentlichen passive Ele-
mente, die Daten speichern, die im Wesentlichen von der Elektronik des
Terminals gespeichert und benutzt werden. Der Kunde dagegen hat
normalerweise keine Möglichkeit, direkt auf die Daten Zugriff zu nehmen, ohne
sich an einen Schalter oder an einen Automaten des betreffenden
10 Finanzinstituts, das die Karte herausgibt, zu begeben. Für den Kunden ist es
also schwierig, die mit der Karte durchgeführten Transaktionen zu kontrollieren
oder darüber Buch zu führen.

Diese Karten enthalten eine Kundenidentifizierung, die es indes nur
erlaubt, die Kunden beim herausgebenden Finanzinstitut identifizieren zu las-
15 sen. Eine Karte kann also normalerweise nur für eine finanzielle Transaktion
benutzt werden, wenn der Kunde und der Terminal-Betreiber beim gleichen
Finanzinstitut affiliert sind. Dagegen ist der Gebrauch der Karte für andere
Arten von Transaktionen - zum Beispiel für nicht finanzielle Transaktionen, für
die aber die zuverlässige Identifizierung des Kunden/Kartenbesitzers benötigt
20 wird - nicht vorgesehen. Für den Kunden ist es also unumgänglich, eine grosse
Anzahl von Karten, für jegliche Arten von finanziellen oder nicht finanziellen
Transaktionen zu besitzen, zum Beispiel mehrere Debit- oder Kreditkarten, die
von verschiedenen Finanzinstituten oder Ladenketten verwaltet werden, oder
Abonnementskarten oder Zugangskarten für geschützte Zonen. Diese Karten
25 sind meistens durch verschiedene Pin-Codes geschützt, die sich der Kunde
mühsam einprägen muss.

Im Falle eines Diebstahles oder einer betrügerischen Handlung mit
der Karte, muss diese gesperrt werden. Die Sperrung kann jedoch erst erfol-
gen, wenn die Karte in ein entsprechendes Gerät eingeführt wird. Die gewöhn-
30 lichen Kreditkarten können jedoch weiterhin in manuell bedienten Apparaten
gebraucht werden; eine sichere Sperrung der Karte ist also nicht möglich.

Ausser Debit- und Kreditkarten kennt man die sogenannten e-cash-Karten (Wertkarten), welche es ermöglichen, Geldbeträge elektronisch zu speichern, welche anschliessend an verschiedenen Terminals als Zahlungsmittel akzeptiert werden. Um diese Karten erneut mit Geldbeträgen 5 versehen zu lassen, muss der Kunde am Schalter oder Automaten eines Finanzinstitutes vorstellig werden, was auch nicht immer möglich ist.

Eine Aufgabe der vorliegenden Erfindung ist es, ein Verfahren oder System vorzuschlagen, das erlaubt, diese Probleme zu vermeiden.

Eine weitere Aufgabe der vorliegenden Erfindung ist es, ein Trans-10 aktionsverfahren vorzuschlagen, das sowohl für finanzielle als auch für nicht finanzielle Transaktionen geeignet ist, und das einfacher und zuverlässiger ist, als die gewöhnlichen Transaktionsverfahren.

Gemäss der vorliegenden Erfindung werden diese Ziele insbesondere durch die Elemente des kennzeichnenden Teils der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem 15 aus den abhängigen Ansprüchen und der Beschreibung hervor.

Insbesondere werden diese Ziele durch ein Transaktionsverfahren zwischen einem Kunden und einem mit einem Telekommunikationsnetz verbundenen Terminal (zum Beispiel ein Point-of-Sale, POS) erreicht, welches die 20 Merkmale der unabhängigen Ansprüche umfasst.

Die vorliegende Erfindung wird mit Hilfe der als Beispiel gegebenen Beschreibung besser verständlich und durch die beiliegenden Figuren veranschaulicht :

Die Figur 1 zeigt ein Blockschema, das den Informationsfluss in einer ersten Ausführungsform des Systems der Erfindung zeigt, wobei der Kunde 25 mit einem Mobilfunktelefon ausgerüstet ist, vorzugsweise ein GSM- oder UMTS-Mobilgerät, das spezielle Kurzmeldungen empfangen und senden kann.

Die Figur 2 zeigt ein Blockschema, das den Informationsfluss in einer zweiten Ausführungsform des Systems der Erfindung zeigt, wobei der Kunde mit einem Mobilfunktelefon ausgerüstet ist, vorzugsweise ein GSM- oder UMTS-Mobilgerät, das spezielle Kurzmeldungen empfangen und senden kann, 5 und wobei das Terminal ein Internet- oder Intranet-taugliches Gerät ist.

Die Figur 3 zeigt ein Flussdiagramm eines Zahlungstransaktionsverfahrens gemäss der Erfindung.

Die Figur 4 zeigt ein Flussdiagramm eines Nachladetransaktionsverfahrens einer SIM-Karte, gemäss der Erfindung.

10 Das auf den Figuren 3 und 4 dargestellte Verfahren kann mit jeder Systemvariante, das beispielsweise in den Figuren 1 und 2 dargestellt ist, ausgeführt werden. Die erste und die zweite Variante benötigen beide ein Mobilfunktelefon mit einer SIM-Karte und einer zusätzlichen infraroten oder induktiven Schnittstelle, die später näher beschrieben wird.

15 Die Figur 1 zeigt den Informationsfluss in einer ersten Ausführungsform der Erfindung. Der Kunde ist mit einem Mobilfunktelefon ausgerüstet, das ein Mobilgerät, zum Beispiel ein GSM- oder UMTS-Mobilgerät 1 und ein Identifizierungsmodul 10, z.B. eine SIM-Karte, umfasst. Die Nummer 11 bezeichnet eine Bedienungseinheit, z.B. eine Tastatur. Der Kunde wird im 20 Mobilfunknetz 6 mit dem Identifizierungsmodul 10 identifiziert. Die SIM-Karte weist einen konventionellen Mikrokontroller 100 auf, welcher in den Kunststoffträger der Karte eingelassen ist und für die GSM-Funktionalitäten der Karte zuständig ist - wie sie zum Beispiel im Artikel « SIM CARDS » von T. Grigorova und I. Leung beschrieben werden, welcher im « Telecommunication 25 Journal of Australia », Vol. 43, No. 2, 1993, auf den Seiten 33 bis 38 erschienen ist - und für neue Funktionalitäten, welche zu einem späteren Zeitpunkt auf die SIM-Karten geladen werden. Die SIM-Karte kann vorzugsweise eine JAVA-fähige Karte sein, d.h. eine Karte mit einem Prozessor, der Instruktionen in der JAVA-Programmiersprache (oder in einer 30 anderen Objekt-orientierten Sprache) ausführen kann. SIM-Karten nach dem Opencard-Konzept von IBM können auch angewendet werden. Die SIM-Karte

weist ausserdem nicht dargestellte Kontaktmittel auf, über welche die Karte mit dem Mobilgerät 1 kommuniziert, in welchem sie eingeführt ist.

Die SIM-Karte weist ausserdem einen zweiten Prozessor 101 (CCI, Contactfree Chipcard Interface) auf, welcher für die kontaktlose Verbindung mit dem POT-Gerät 2 zuständig ist. Der zweite Prozessor führt unter anderem die weiter unten beschriebenen TTP (Trusted Third Party)-Funktionen aus, um chiffrierte und signierte Meldungen zu empfangen und zu senden. Eine logische Schnittstelle 102 verbindet die beiden Prozessoren 101 und 102. Optional könnte ein einziger Prozessor diese beiden Prozessoren 101, 102 ersetzen.

Die kontaktlose Schnittstelle mit dem Terminal 2 kann beispielsweise mindestens eine in der SIM-Karte integrierte und mit dem zweiten Prozessor 101 verbundene Spule aufweisen (nicht dargestellt), mit der Daten in beiden Richtungen über eine Funkstrecke induktiv übertragen werden. Eine induktive Spule kann in einer Variante auch im Gehäuse des Mobilgeräts integriert werden. In einer weiteren Variante umfasst die kontaktlose Schnittstelle einen infraroten Sender-Empfänger an die Gehäuse des Mobilgeräts. In einer noch weiteren Variante ist die kontaktlose Schnittstelle in einem Erweiterungsmodul integriert, das entfernbar mit dem Mobilgerät verbunden werden kann. Die kontaktlose Kommunikation zwischen den beiden Geräten wird vorzugsweise verschlüsselt, zum Beispiel mit einem DEA-, DES-, TDES-, RSA- oder ECC-Sicherheitsalgorithmus.

Die kontaktlose Kommunikation ist vorzugsweise auf einem benannten Standard basierend, zum Beispiel auf dem IrDA-Protokoll (Infrared Data Association). Fehlerprüf- und Fehlerkorrekturmittel werden vorzugsweise für diese Kommunikation angewendet. Vorzugsweise werden ausserdem Endgerätidentifizierungsmittel angewendet, um eine Verbindung mit nur einem bestimmten Endgerät zuverlässig zu etablieren, falls mehrere Endgeräte, z.B. mehrere Mobilgeräte und/oder mehrere Terminals, in einem Raum vereinigt sind.

Bei einer induktiven Signalübermittlung vom Terminal zur Chipkarte wird vorzugsweise ein Phasenmodulations-Verfahren eingesetzt, während in

der umgekehrten Richtung vorzugsweise die Amplitude der Signale moduliert wird.

Die SIM-Karte enthält vorzugsweise ein Sonderfeld IDUI (International Debit User Identification), mit dem der Kunde vom Terminal-
5 Betreiber und/oder von einem Finanzinstitut identifiziert wird. Die Identifizierung IDUI wird vorzugsweise in einem ersten gesicherten Speicherbereich eines der beiden Prozessoren 101, 102 gespeichert. Die IDUI enthält mindestens eine Identifizierung vom Netzbetreiber, eine Benutzernummer, die ihn von anderen Kunden beim selben Netzbetreiber
10 identifiziert, eine Benutzerklassenangabe, die definiert, welche Dienste er benutzen darf, und optional noch eine Landidentifizierung. Außerdem enthält die IDUI Sicherheitsdaten, unter anderem einen Transaktionszähler Tz, ein Lade-Token LT_c, und ein Time-Out-Feld TO, das die Validierungszeit angibt. Die Funktion von diesen verschiedenen Daten wird später erläutert.

15 Die SIM-Karte enthält außerdem einen zweiten, gesicherten Speicherbereich, in welchem elektronische Geldeinheiten (Geldbeträge) gespeichert werden können.

Das symbolisch dargestellte Terminal 2 ist ebenfalls mit einem kontaktlosen Sender-Empfänger 20 versehen, zum Beispiel mit einer induktiven
20 Spule oder mit einem infraroten Sender-Empfänger. Dank dieser Schnittstelle kann das Mobilsystem 1,10 kontaktlos mit dem Gerät 2 in beiden Richtungen kommunizieren.

Das Terminal 2 kann zum Beispiel ein speziell mit einer Funkschnittstelle 20 ausgerüsteter Point-of-Sale (POS) in einem Geschäft sein
25 und wird mit einem Sonderfeld POSID (Point Of Sale Identification) identifiziert. Die POSID hängt von der Anwendung ab ; im Falle einer Geschäftskasse enthält sie eine Identifizierung vom Netzbetreiber, eine Areaidentifizierung (Teilgebiet in einem Land), eine POS-Nummer, die ihn von anderen POS beim selben Netzbetreiber identifiziert, eine POS-Klassenangabe, die definiert, welche Dienste er benutzen oder anbieten darf, das Datum, die Zeit, die benutzte Währung (SDR, Euro oder Dollars) und optional noch eine Landesidentifizierung.

Das Terminal 2 wird vorzugsweise mit nicht dargestellten Dateneingabe-Mitteln versehen, zum Beispiel mit einer Tastatur, und mit nicht dargestellten Datenanzeige-Mitteln, zum Beispiel mit einem Bildschirm.

Die IDUI-Identifizierung wird dem Terminal über die kontaktlose

- 5 Schnittstelle 10/101 übertragen, und im Terminal mit der POSID und mit dem erfassten Transaktionsbetrag A, verknüpft, so dass ein elektronischer Transaktionsbeleg entsteht, der mit einem TTP (Trusted Third Party)- oder PTP (Point-to-Point)-Prozess verschlüsselt und signiert wird.

Der Transaktionsbeleg wird dann über ein nicht dargestelltes

- 10 Modem und durch das Kommunikationsnetz 5, zum Beispiel durch ein öffentliches vermitteltes Fernsprechnetz an die ebenfalls mit dem Netz 5 verbundene Clearingeinheit 3 übermittelt. Diese empfängt die elektronischen Belege von verschiedenen Terminals 2, unabhängig vom Land oder Verkehrsbereich, und unabhängig vom Land oder Finanzinstitut des Kunden. In der Clearingeinheit 3
- 15 werden diese Transaktionsbelege nach Finanzinstitut, eventuell auch nach Operator, geordnet und dem Dienstzentrum 4, 4', 4'' des entsprechenden Finanzinstitutes zugestellt. Clearingeinheiten an sich sind in der GSM-Technik schon bekannt und werden beispielsweise für das Sammeln und für die Weiterverteilung von Verbindungskosten verwendet. Die Clearingeinheit kann
- 20 beispielsweise eine Datenbank enthalten, die angibt, mit welchem Finanzinstitut der vorher mit seinem IDUI identifizierte Kunden affiliert ist.

Die durch die Clearingeinheit 3 behandelten elektronischen Transaktionsbelege werden an das Dienstzentrum 4, das vorzugsweise über einen Finanzserver verfügt, weitergeleitet. Im Finanzserver werden die eingereichten

- 25 Transaktionsbelege zuerst entschlüsselt und in einem Zwischenspeicher 43 gespeichert. Ein Abgleichmanagement-Modul 42 schreibt dann den vom Kunden signierten Transaktionsbetrag den entsprechenden Bankkonten 420, 420' und/oder 420'' des Terminal-Betreibers gut. Diese Konten können durch dasselbe oder durch ein anderes Finanzinstitut verwaltet werden. Das
- 30 Abgleichmanagement-Modul führt außerdem Kontrollbuchungen zum Konto des Kunden durch. Entsprechend wird das Kontrollkonto 41 des Kunden beim Finanzinstitut belastet, oder werden die Transaktionsdaten für eine spätere Kontrolle gespeichert. Der Finanzserver enthält außerdem einen TTP-Server

40, um Belege und Meldungen mit dem TTP (Thrusted Third Party)-Algorithmus zu chiffrieren und zu signieren. Ausserdem ist jeder Finanzserver 4 mit einem SIM-Server 70 verbunden, zum Beispiel mit einem SICAP-Server. Das SICAP-Verfahren wurde unter anderem im Patent EP689368 beschrieben, 5 und erlaubt, Dateien, Programme und auch Geldbeträge zwischen dem SICAP-Server 70 und der SIM-Karte 10 im Mobilgerät 1 über das öffentliche GSM-Netz 6 auszutauschen (Pfeil 60). Andere Übertragungsprotokolle können auch für die Datenübertragung zwischen dem SIM-Server und den SIM-Karten angewendet werden. Dadurch kann beispielsweise Geld auf der SIM-Karte 10 10 nachgeladen werden, wie später näher beschrieben. Der SIM-Server 70 ermöglicht ausserdem die gesteuerte Kommunikation zwischen dem Kunden und dem TTP-Server 40 beim Finanzinstitut.

Die Figur 2 zeigt den Informationsfluss in einer zweiten Ausführungsform der Erfindung. Der Kunde ist ebenfalls in dieser Variante mit einem 15 Mobilfunktelefon ausgerüstet, zum Beispiel mit einem GSM-Funktelefon 1 mit einer SIM-Karte, vorzugsweise mit einer SICAP-tauglichen SIM-Karte und/oder mit einer JAVA-tauglichen Karte. Ebenfalls ist eine induktive oder infrarote Schnittstelle im Mobilsystem 1 enthalten, mit der eine kontaktlose Verbindung mit dem Terminal 2 durchgeführt werden kann. Daten und/oder Programme 20 können auf diese Weise in beiden Richtungen zwischen dem Terminal 2 und der SIM-Karte 10 im Mobilsystem ausgetauscht werden.

Das Terminal 2' ist aber in diesem Fall ein Rechner, der vorzugsweise mit einem Netz, zum Beispiel im Internet oder einem Intranet, verbunden ist. Verschiedene Informationen oder Angebote, zum Beispiel Produkt-Angebote, 25 können beispielsweise mit einem geeigneten Menü auf dem Bildschirm des Rechners 2 offeriert werden. Der Kunde kann diesen Rechner mit seinem Mobilgerät steuern. Beispielsweise kann er die Position eines Cursors in einem Menü von zum Verkauf angebotenen Produkten oder Informationen durch Be-tätigen der Cursor-Verschiebetasten auf der Tastatur 11 seines Mobiltelefons 30 steuern. Die Cursor-Verschiebeinstruktionen werden über die kontaktlose Schnittstelle 101, 20 zum Rechner 2' gesendet. Der Benutzer betätigt eine Bestätigungstaste, zum Beispiel die Taste # auf seiner Tastatur, um die ausgewählte Menüoption zu bestätigen, zum Beispiel um ein Produkt zu bestellen.

Die im Mobilgerät 1,10 gespeicherte Kundenidentifizierung wird mit der POSID und mit dem der angewählten Menüoption entsprechenden Transaktionsbetrag in einem elektronischen Transaktionsbeleg verknüpft, TTP- oder PTP-verschlüsselt und signiert. Der Transaktionsbeleg enthält vor-
5 zugsweise eine aus der SIM-Karte 10 gewonnene Kundenidentifizierung IDUI, eine der angewählten Menüoption entsprechende Lieferantenidentifizierung, und eine der angewählten Menüoption entsprechende Produktidentifizierung, vorzugsweise im Flexmart-Format wie in der Patentanmeldung
PCT/CH96/00464 vorgeschlagen. Dieser Beleg wird durch ein Flexmart-Modul
10 21 ermittelt. Das Flexmart-Modul ist vorzugsweise eine vom Rechner 2' ausgeführte Software-Anwendung.

Analog zur ersten Ausführungsform wird dann der elektronische Transaktionsbeleg an den entsprechenden Finanzserver 4, 4' oder 4" durch die Clearingeinheit 3 übermittelt und dort verarbeitet.

15 Ein Zahlungstransaktionsverfahren wird jetzt mit Hilfe der Figur 3 näher beschrieben. Dieses Verfahren kann auf beliebige Ausführungsformen der Erfindung gemäss den Figuren 1 und 2 angesetzt werden. Dieser Ablauf ist jedoch allgemein gültig und nicht auf GSM- oder UMTS-Prozesse beschränkt.

Die erste Kolonne in Figur 3 zeigt die Verfahrensschritte, die haupt-
20 sächlich das Mobilfunktelefon 1 des Kunden involvieren ; die zweite beschreibt die Verfahrensschritte, die vom Terminal 2 ausgeführt werden ; die dritte betrifft die Operationen vom Dienstzentrum 4 und die vierte die Effekte auf die ver-
schiedenen Konten beim Finanzinstitut. Es muss aber bemerkt werden, dass viele Verfahrensschritte entweder mit dem Mobilfunktelefon 1, zum Beispiel als
25 Prozess innerhalb der SIM-Karte 10 oder im Terminal 2 ausgeführt werden können. Zum Beispiel kann die Dateneingabe entweder mit dem Terminal oder mit dem Mobilfunktelefon 1 erfolgen, wenn dieses eine Tastatur enthält, wie zum Beispiel ein GSM-Mobilgerät.

Dieses Verfahren setzt im Schritt 200 voraus, dass die Identifizie-
30 rungskarte 10 des Kunden einen gesicherten Speicherbereich umfasst, in welchem elektronische Geldeinheiten gespeichert werden. Wertkarten sind an sich schon bekannt ; wir werden später in Bezug auf Figur 4 näher erläutern,

wie der Geldbetrag nachgeladen werden kann. Ausserdem beschreibt die Patentanmeldung EP96810570.0 ein Verfahren, um SIM-Karten mit einem Geldbetrag nachzuladen.

Das Mobilsystem 1 bzw. 10 wird im Schritt 201 funktionsbereit geschaltet, zum Beispiel mit dem Einschalten des Mobilgerätes. Ebenso wird im Schritt 202 das Terminal 2 aktiviert. Das Terminal 2 ruft dann im Schritt 203 in einem Broadcastverfahren den nächsten, unbestimmten Kunden auf (Kartenpaging).

Wenn die Verbindung zwischen dem Terminal 2 und dem Mobilfunktelefon 1, 10 hergestellt worden ist, übergibt im Schritt 204 das Mobilfunktelefon dem Terminal seine Identifizierung IDUI (International Debit User Identification) und die Bestätigung, dass er solvent ist. Die IDUI ist in einem ersten gesicherten Bereich der Karte abgelegt. Ob die Solvenz ausreicht, kann in diesem Moment noch nicht entschieden werden.

Das Terminal 2 enthält eine vorzugsweise vom Finanzserver 4 periodisch aktualisierte Schwarzliste über zu sperrende Kunden. Die vom Kunden übermittelte IDUI wird mit der Schwarzliste verglichen (Schritt 205) (Erlaubnisdaten). Wenn die vom Kunden übergebene IDUI in der Schwarzliste gefunden wird (Schritt 206), wird ein Blockierflag im Schritt 207 gesetzt. Wenn keine Übereinstimmung gefunden wird, kann auf der Tastatur des Terminals 2 der Transaktionsbetrag A eingegeben werden. In einer Variante kann der Transaktionsbetrag A auch mit den Eingabemitteln 11 des Mobilgeräts 1 eingegeben werden. Das Terminal 2, oder in einer Variante die SIM-Karte 10, verknüpft dann diesen Betrag mit der Identifizierung des Terminals 2 und der IDUI und sendet dem Kunden diesen Belastungsbeleg. Vorzugsweise wird ausserdem noch eine Referenzwährung, wie zum Beispiel SDR, Euro oder Dollar, eingeschlossen.

Da die Kommunikation signiert wird, kann im Schritt 210 geprüft werden, ob der Belastungsbeleg mit der IDUI korreliert. Wenn nicht, wird der Rückweisungsgrund am Terminal 2 angezeigt (Schritt 223). Sonst wird im Schritt 211 ein Blockierflag geprüft. Ist es gesetzt (212), erfolgt ein Check-up mit dem Finanzserver 4 (Schritt 248). Ist er nicht gesetzt, erfolgt ein Area-

Check-up (Schritt 213). Es können dadurch SIM-Karten je nach Benutzungs-Area gesperrt werden. Wenn der Area Check-up negativ ist, erfolgt ein Check-up mit dem Finanzserver 4 (Schritt 248) ; sonst wird ein Time-Out Check-up gemacht (Schritt 215). Es wird geprüft, ob die Validationszeit, während der

- 5 Transaktionen ohne Checkup durchgeführt werden können, schon abgelaufen ist. Ist die Validationszeit abgelaufen (216), erfolgt ein Check-up mit dem Finanzserver (Schritt 248) ; sonst wird der Kunde im Schritt 217 aufgefordert, sein Benutzerpasswort am Mobilgerät 1 manuell einzugeben. Ist das eingegebene Passwort korrekt (Schritt 218), wird der Betrag A gegebenenfalls in die
- 10 Einheitswährung (zum Beispiel SDR) umgerechnet (Schritt 219). Damit wird ein internationaler Einsatz des Konzepts ermöglicht. Sonst wird im Schritt 223 auf dem Terminal 2 die Rückweisung mit Grundangabe angezeigt.

Das Mobilfunktelefon 1/10 prüft dann im Schritt 220, ob der zu belastende Transaktionsbetrag A mit dem im zweiten Speicherbereich geladenen

- 15 Geldbetrag gedeckt ist (Solvenzprüfung). Wenn dies nicht der Fall ist, wird am Bildschirm des Terminals dieser Rückweisungsgrund angezeigt (Schritt 223).

Wenn alle diese Prüfungen erfolgt sind, wird im Schritt 222 die Transaktion mit einem Transaktionszähler Tz gezählt, der inkrementiert wird.

- 20 Dieser Zähler entspricht der Anzahl der mit der Karte 10 abgelaufenen Transaktionen. Im Schritt 224 werden dann der Transaktionsbetrag A, die Terminal-Identifizierung POSID und die Benutzeridentifizierung IDUI in einem Transaktionsbeleg verknüpft, welcher zusätzlich zertifiziert und optional verschlüsselt und eventuell noch komprimiert wird. Das ECC-Verfahren (Elliptic Curve Cryptosystem) kann beispielsweise für die Zertifizierung angewendet
- 25 werden. Ein geeignetes Zertifizierungs- und Verschlüsselungsverfahren wird später als Beispiel näher erläutert.

Der belastete Transaktionsbetrag A wird dann im Schritt 225 auf dem gespeicherten Geldbetragskonto abgebucht und der Transaktionsbeleg wird im Schritt 226 in einem Stack auf dem Identifizierungsmodul 10 abgelegt.

- 30 Dieser Kartenstack beim Kunden kann nach Bedarf zwecks detaillierter Kontrolle vom Finanzserver 4 abgerufen werden. Vorzugsweise kann der

Kunde selber die im Stack gespeicherten Transaktionsbelege auf seinem Mobilgerät 1 anzeigen.

Nach dem Schritt 224 wird der Transaktionsbeleg dem Terminal 2 zur Abrechnung übergeben, und die Kundensignatur wird vom Terminal geprüft

5 (Schritt 227). Optional wird im Schritt 228 ein Papierbeleg am Terminal für den Kunden ausgedruckt.

Im Schritt 229 wird dann im Terminal 2 der Belastungsbeleg mit eventuell zusätzlichen Daten verknüpft, und der Transaktionsbeleg wird vom Terminal 2 elektronisch signiert und optional komprimiert und chiffriert. Der auf 10 diese Weise vorbereitete elektronische Transaktionsbeleg wird dann optional im Schritt 230 in einem Stack im Terminal 2 abgelegt. Der Stack enthält Transaktionsbelege von verschiedenen Kunden. Die Transaktionsbelege werden dann individuell oder gruppiert während dem Schritt 231 der Clearingeinheit 3 übertragen. Die Übertragung kann entweder gleich nach der 15 Transaktion erfolgen, oder es können in periodischen Zeitabständen (zum Beispiel jede Stunde oder jeden Tag) mehrere Transaktionsbelege aus dem Stack übertragen werden. Ein Batch-Prozess, um alle Transaktionsbelege zum Beispiel in der Nacht zu übertragen, kann auch angewendet werden.

Die Clearingeinheit 3 empfängt individuelle oder gruppierte Trans- 20 aktionsbelege aus mehreren Terminals 2 in derselben geographischen Zone (Schritt 234). Mehrere geographisch verteilte Clearingseinheiten können vorgesehen werden. Im Schritt 235 teilt die Clearingseinheit 3 die von verschiedenen Terminals empfangenen Transaktionsbelege den entsprechenden Finanzinstituten oder Dienstanbietern zu, und leitet diese Transaktionsbelege 25 entsprechend weiter.

Wenn die Transaktionsbelege chiffriert sind, müssen sie von der Clearingeinheit zuerst entschlüsselt werden, um einem Finanzserver 4, 4', 4" 30 zugeteilt zu werden, und dann wieder von der Clearingseinheit chiffriert, um sie weiterzuleiten. In einer bevorzugten Variante werden jedoch die Datenelemente in den Feldern IDUI und eventuell POSID des Transaktionsbeleges, die für das Clearing benötigt sind, vom Terminal 2 nicht chiffriert. Dadurch kann

eine gesicherte, end-to-end verschlüsselte Übertragung der Transaktionsbelege zwischen den Terminals und den Finanzservern 4, 4', 4'' erreicht werden.

Der zuständige Finanzserver empfängt im Schritt 236 die Transaktionsbelege, und der TTP-Server 40 dekomprimiert und entschlüsselt sie (falls benötigt), und überprüft die Echtheit der Signaturen vom Terminal 2 und vom Identifizierungsmodul 10. Im Schritt 237 wird geprüft, ob der POSID und/oder die IDUI sich in einer Revocation List befinden. Ist der Test positiv (238), weil weder die Terminalidentifizierung noch die Kundenidentifizierung IDUI sich auf dem Revocation List befinden, erfolgt im Schritt 239 ein Test des Ladetokens

- 5 benötigt), und überprüft die Echtheit der Signaturen vom Terminal 2 und vom Identifizierungsmodul 10. Im Schritt 237 wird geprüft, ob der POSID und/oder die IDUI sich in einer Revocation List befinden. Ist der Test positiv (238), weil weder die Terminalidentifizierung noch die Kundenidentifizierung IDUI sich auf dem Revocation List befinden, erfolgt im Schritt 239 ein Test des Ladetokens
- 10 LT. Der Ladetoken LT gibt die Anzahl der Nachladungen der Karte 10. Dieser Ladetoken wird im Finanzserver (LT_s) und im Identifizierungsmodul 10 (LT_c) nach jedem Nachladeprozess aktualisiert, wie später beschrieben. Eine Kopie des Ladetokens LT_c ist im Feld IDUI im Transaktionsbeleg übertragen. Der vom Mobilfunktelefon 1,10 mitgeteilte Ladetoken LT_c muss gleich wie der im
- 15 Finanzserver 4 gespeicherte Ladetoken LT_s sein. Falls Nachladebelege noch auf dem Weg zwischen der Finanzserver 4 und dem Mobsystem 1,10 sind, kann LT_c temporär auch kleiner sein als LT_s . Der Finanzserver 4 prüft also ob $LT_c \leq LT_s$.

Wird im Schritt 240 diese Bedingung nicht verifiziert, wurde wahrscheinlich ein nicht autorisierter Nachladeprozess durchgeführt und das Verfahren geht zum Schritt 241 über. Es wird hier unterschieden, ob die Fälschung vom Terminal oder vom Kunden gemacht worden ist. Ist der Kunde verantwortlich, wird er im Schritt 242 in einer Schwarzliste eingetragen. Ein Kundensperrungsbeleg wird vorzugsweise generiert und an das

- 20 Mobilfunktelefon 1, 10 des Kunden geschickt, um das Blockierflag zu setzen und dieses System zu sperren, sowie an alle Terminals oder zumindest an alle Terminals im einem vordefinierten geographischen Bereich, um diesen Kunden in der Schwarzliste dieses Terminals einzutragen. Wurde dagegen das Problem vom Terminal verursacht, wird dieses im Schritt 243 in einer Terminal-
- 25 Schwarzliste eingetragen.
- 30 Schwarzliste eingetragen.

Wird im Schritt 240 die Ladetokenprüfung bestanden, kann im Schritt 244 der Transaktionsbetrag A im Transaktionsbeleg einem

Kundenprüfkontos 41 beim Finanzinstitut belastet werden. Im Schritt 245 wird entsprechend der Transaktionsbetrag A einem Konto 420, 420' oder 420" des Terminal-Betreibers bei einem Finanzinstitut gutgeschrieben. Bearbeitungsgebühren können auch von einem Finanzinstitut und/oder vom Terminalbetreiber 5 oder vom Netzoperator dem Konto 420 und/oder einem Kundenkonto belastet werden.

Im Schritt 246 trägt dann der Finanzserver 4 diese Transaktion in den Transaktionszähler ein. Ein Prozess erfolgt dann im Schritt 247, um die Werte vom Ladetoken LT_c und vom Transaktionszähler Tz im Mobilfunktelefon 10 zu aktualisieren

Wir kommen auf den Prozess im Mobilfunktelefon 1, 10 zurück. Wie schon erklärt, gelangt diese Einrichtung zum Schritt 248, wenn ein Sicherheitsproblem im Schritt 212, 214 oder 216 festgestellt wird. In diesem Fall erfolgt ein kompletter Checkup mit dem Finanzserver, vorzugsweise über das 15 Mobilfunknetz 6. Der Checkup umfasst zum Beispiel einen Test und eine Erneuerung des Authentifizierungszertifikats sowie eine Überprüfung von allen ausgeführten Parametern, zum Beispiel der Ladetoken LT, der Transaktionszähler Tz, der Blackliste, usw. Ist das Ergebnis des Checkups negativ (Schritt 249), wird das Blockierflag gesetzt, so dass das Mobilsystem 1, 20 oder mindestens die betreffende Anwendung in der SIM-Karte 10, gesperrt wird (Schritt 253). Zeigt im Gegenteil diese Prüfung, dass höchstwahrscheinlich keine Fälschung versucht wurde, wird im Schritt 250 die Validationszeit neu gesetzt. Mit der Validationszeit kann zum Beispiel ein Identifizierungsmodul gesperrt werden, wenn es während einer vordefinierten Zeit, zum Beispiel ein 25 Jahr, nicht benutzt wird. Diese Angabe muss daher nach jeder Benutzung neu eingestellt werden. Der Blockierflag wird dann im Schritt 251 gelöscht, und, wenn nötig, eine neue Area im Schritt 252 gesetzt.

Wichtig zu bemerken ist, dass der Belastungsprozess mit unterschiedlichen Währungen erfolgen kann, zum Beispiel auf der Basis der im 30 Telekommunikationsbereich üblichen SDR (Sonderziehungsrechte) oder mit einer anderen Referenzwährung (zum Beispiel Euro oder Dollar). Der maximale Betrag auf der Karte ist je nach Kundenklasse definiert. Minimal ist ein

Defaultwert in SDR möglich. Jedes Terminal 2 speichert den für ihn relevanten SDR-Wert (z.B. währungsspezifisch), der ihm im Einbuchungsprozess vom Server mitgeteilt wird. Je nach Kursschwankungen werden die Terminals vom Finanzserver automatisch mit aktuellen Kursen versorgt.

5 Ein Verfahren zum Nachladen des Mobilsystems 1, 10 mit einem Geldbetrag wird jetzt mit Hilfe der Figur 4 näher beschrieben. Dieses Verfahren kann ebenfalls auf beliebige Ausführungsformen der Erfindung gemäss den Figuren 1 oder 2 angesetzt werden.

Ein Nachladeprozess erfolgt in diesem Beispiel mit dem

10 Mobilfunktelefon 1,10 des Kunden und dem Terminal 2 zusammen. Es wäre jedoch auch möglich, den Geldbetrag auf dem Identifizierungsmodul 10 mit einer Transaktion, die nur das Mobilfunktelefon 1,10 und das Dienstzentrum 4 betrifft, durchzuführen. Diese Lösung hätte den Vorteil, das der Kunde sich nicht an einem Terminal begeben muss; gewisse Sicherheitsprüfungen können

15 jedoch in diesem Fall nicht durchgeführt werden. Diese Variante wird daher vorzugsweise nur angewendet, um kleinere Geldbeträge zu übertragen oder wenn zusätzliche Sicherheitsmechanismen vorgesehen sind. Ein direkter Nachladeprozess vom Finanzserver 4 könnte aber auch angesetzt werden. Je nach Kundenklasse, oder auch nach Bedarf, kann vom Finanzserver der

20 Beleg-Kartenstack beim Kunden, zwecks detaillierter Kontrolle, abgerufen werden. Nach dem Nachladeprozess kann der Stack vom Finanzserver gelöscht werden.

Die erste Kolonne in Figur 4 zeigt die Verfahrensschritte, die hauptsächlich das Mobilfunktelefon 1,10 involvieren ; die zweite beschreibt die

25 Verfahrensschritte, die vom Terminal 2 ausgeführt werden; die dritte betrifft die Operationen vom Dienstzentrum 4 und die vierte die Effekte auf die verschiedenen Konten beim Finanzinstitut. Es muss aber bemerkt werden, dass viele Verfahrensschritte entweder mit dem Mobilfunktelefon 1, 10, zum Beispiel innerhalb der SIM-Karte 10, oder mit dem Terminal 2 ausgeführt

30 werden können. Zum Beispiel können die Verfahrensschritte, welche die Dateneingabe betreffen, entweder auf dem Terminal oder auf dem Mobilgerät 1 ausgeführt werden, wenn das Mobilgerät eine Bedienungseinheit enthält. Die

Kommunikation zwischen den beiden Teilen wird vorzugsweise verschlüsselt, zum Beispiel mit einem DEA-, DES-, TDES-, RSA- oder ECC-Sicherheitsalgorithmus.

Im Schritt 300 wird zuerst das Mobilfunktelefon 1,10, operativ für den

5 Nachladeprozess freigeschaltet ; das Terminal 2 wird seinerseits auch im Schritt 301 aktiviert. Das Terminal 2 ruft dann im Schritt 302 in einem Broadcastverfahren das nächste, unbestimmte Mobilsystem 1,10 auf (« Kartenpaging »).

Wenn die Verbindung zwischen dem Terminal 2 und dem Mobilfunktelefon 1,10 hergestellt worden ist, übergibt im Schritt 303 der Kunde dem

10 Terminal seine Identifizierung IDUI (International Debit User Identification) und den Typ des zu startenden Prozesses, hier eine Nachladung.

Das Terminal 2 enthält eine vorzugsweise vom Finanzserver 4 periodisch aktualisierte Schwarzliste über zu sperrende Mobilsysteme (Revocation list). Die vom Kunden übermittelte IDUI wird mit der Schwarzliste verglichen (Schritt 304). Wenn die vom Kunden übergebene IDUI in der Schwarzliste gefunden wird (Schritt 305), wird ein Blockierflag im Schritt 306 gesetzt. Danach, oder wenn keine Übereinstimmung gefunden wird, wird im Schritt 307 geprüft, ob die Aufforderung mit der IDUI korreliert. Wenn nicht, wird der

15 Rückweisungsgrund am Terminal 2 angezeigt (Schritt 315). Sonst wird im Schritt 308 das Blockierflag geprüft. Ist es gesetzt, wird das Mobilfunktelefon 1, 10, oder mindestens die betreffende Anwendung in der Identifizierungskarte 10, gesperrt (Schritt 331). Ist es nicht gesetzt, wird der Kunde im Schritt 310 aufgefordert, sein Benutzerpasswort am Mobilgerät 1 manuell einzugeben. Ist

20 das eingegebene Passwort nicht korrekt (Schritt 311), wird ebenfalls das Blockierflag gesetzt und der Rückweisungsgrund am Terminal 2 angezeigt (Schritt 315) ; sonst ist der Prozess frei für die Nachladung und der Kunde wird im Schritt 312 aufgefordert, einen Nachladebetrag A einzugeben. In der dargestellten Variante kann der Nachladebetrag am Terminal 2 eingegeben

25 werden ; dieser Betrag wird im Schritt 313 mit der POSID und mit der IDUI verknüpft, signiert und an die Karte 10 übermittelt. Der Betrag A könnte aber

30

auch am Mobilgerät 1 erfasst werden ; in diesem Fall ist kein Terminal involviert und die POSID wird daher nicht benötigt.

Im Schritt 314 wird geprüft, ob die IDUI in den vom Terminal 2 empfangenen Daten mit der eigenen IDUI übereinstimmt. Wenn nicht, wird der 5 Rückweisungsgrund am Terminal 2 angezeigt (Schritt 315) ; sonst wird der gewünschte und am Terminal eingegebene Nachladebetrag auf dem Bildschirm des Mobilgeräts 1 angezeigt. Im Schritt 316 werden dann die POSID (optional), die IDUI, die schon erwähnte Anzahl Zahlungstransaktionen Tz, die 10 auf der Karte gespeicherte Anzahl ausgeführter Nachladeprozesse (LTc, Lade- Token Kunden) und der Restbetrag auf der Karte DRA (Debit Rest Amount) verknüpft, signiert, verschlüsselt und dann optional komprimiert. Es entsteht dadurch ein Nachladebeleg. Optional kann auch der Beleg-Stack auf der Karte übermittelt werden, zum Beispiel je nach Kundenklasse, bei Kartenausgabe 15 oder nach Bedarf während der Nutzung bei Solvenzproblemen. Die POSID wird nur in den Nachladebeleg integriert, wenn der Kunde über ein Mobilgerät ohne geeignete Eingabemittel verfügt. Der Nachladebeleg wird dann an den Finanzserver 4, 4', bzw. 4" durch das Netz 6 übermittelt, wo der TTP-Server 40 diesen Beleg im Schritt 317 empfängt, gegebenenfalls entschlüsselt und dekomprimiert, und die Signatur vom Kunden und gegebenenfalls vom 20 Terminal überprüft.

Im Schritt 319 werden mit Hilfe der Tabelle 318, welche die Anzahl und Token bezüglich der Prozesse zwischen dem Kunden und dem Finanzserver speichert, folgende Prüfungen durchgeführt :

Beträgeprüfung : Die Summe ΣA aller auf dem Identifizierungsmodul 25 10 geladenen Beträge, inklusive der Startsumme, muss gleich oder kleiner sein als die Summe aller Kontrollbelastungen ΣKB und des Restbetrags DRA auf dem Identifizierungsmodul. Die Summe kann kleiner sein, weil die Belege, die noch zwischen dem Mobilfunksystem 1,10, der Clearingeinheit 3 und dem Finanzserver 4, 4', 4" sind, in diesem Moment noch nicht erfasst werden 30 können.

Ladetoken-Prüfung : Die Anzahl von Lade- bzw. Nachlade-Transaktionen wird im Mobilfunktelefon, zum Beispiel in der SIM-Karte mit einem Token LTC und im Finanzserver 4 mit einem anderen Token LTS gezählt. Diese beide Token müssen gleich sein.

5 Transaktionszählerprüfung : Für jede Zahlungstransaktion wird der Transaktionszähler T_z im Mobilfunktelefon 1,10 inkrementiert ; in jedem Nachladebeleg wird auch T_z übertragen. Der beim Finanzserver gespeicherte Transaktionszähler T_{zs} , der durch die vom Kunden transferierten Belege inkrementiert wird, muss gleich oder eventuell kleiner sein als der
10 Transaktionszähler T_z im Mobilfunktelefon 1,10.

Wenn eine dieser drei Bedingungen nicht erfüllt ist (Schritt 320), wird der Blockierflag im Schritt 321 gesetzt und der Nachladeprozess im Schritt 325 zurückgewiesen. Sonst wird im Schritt 322 der Kontostand 41 des Kunden überprüft. Reicht er nicht für die Nachladung, wird im Schritt 325 ebenfalls die Rückweisung aufbereitet.

Wenn das Konto (oder die Kontolimite) des Kunden beim Finanzinstitut 4 für den nachzuladenden Betrag reicht (Schritt 322, 323), wird dieser Betrag bei einem Kundenkonto des Finanzinstitutes abgehoben (324), inklusive allfälliger Kommissionen. Gleichzeitig wird auf dem Prüfkonto 41 der geforderte Nachladebetrag gebucht. Ein Nachladebeleg wird dann im Schritt 326 aus der POSID, der IDUI, dem Betrag A, dem neuen Lade-Token LTn, und einem vordefinierten Time Out Inkrement TOi erstellt. Dieser Nachladebeleg wird im Schritt 327 signiert, optional verschlüsselt und komprimiert, und an das Mobilsystem 1,10 des Kunden übertragen. Dieses prüft während dem Schritt 328, ob die Signatur im Beleg vom Finanzserver stammt, und verifiziert während dem Schritt 329, ob das Blockierflag gesetzt ist. Falls es gesetzt ist (Schritt 330), wird das Mobilfunktelefon 1, oder mindestens die betreffende Anwendung, im Schritt 331 gesperrt. Sonst wird noch geprüft, ob der Finanzserver eine Rückweisung aufgefordert hat (Schritt 332), was zur Unterbrechung des Prozesses mit Anzeige des Rückweisungsgrundes führt (Schritt 334).

Wenn alle Tests erfolgreich bestanden sind, wird im Schritt 335 das Kartenkonto mit dem geforderten Nachladebetrag gebucht. Der alte Ladetoken LTc wird dann mit dem vom Finanzserver übermittelten neuen Ladetoken LTn ersetzt (Schritt 336), der Transaktionszähler Tz auf der Karte wird im nächsten 5 Schritt 337 zurückgesetzt, und der Time Out TOi im Schritt 338 neu gesetzt. Wenn im Schritt 339 festgestellt wird, dass im Nachladabeleg das POSID enthalten ist, wird ausserdem im Schritt 340 eine neue Area gesetzt.

Der Nachladebetrag wird dann als Bestätigung angezeigt, entweder am Bildschirm des Mobilgeräts oder am Terminal (Schritt 341). Schliesslich 10 wird auch noch der Gesamtkontostand auf der Karte angezeigt (Schritt 342).

In dem mit Hilfe der Figuren 3 und 4 beschriebenen Beispiel wird das „reale“ Bankkonto des Kunden beim Finanzinstitut schon bei der Nachladung der Karte belastet. Andere Zahlungsvarianten, zum Beispiel mit Kreditkarte oder durch Erstellung einer Rechnung, sind natürlich im Rahmen 15 dieser Erfindung auch möglich. In einer Variante kann das System auch als Kreditsystem funktionieren: in diesem Fall wird das Bankkonto des Kunden erst belastet, wenn der Finanzserver 7 einen Transaktionsbeleg empfängt. Der im zweiten Speicherbereich der Karte gespeicherte Geldbetrag nützt in diesem Fall nur als Ausgabelimit.

20 Die Sicherung der Datenübermittlungen durch Kryptographie wird in zwei verschiedenen Segmenten unterschiedlich unternommen. Zwischen dem Kunden und dem Terminal wird die Kommunikation durch die Luftschnittstelle durch zum Beispiel einen Algorithmus wie DES, TDES, RSA oder ECC sichergestellt. Zwischen Kunden und Finanzserver kommt dagegen das TTP (Trusted Third Party)- Verfahren, oder optional ein PTP-Verfahren (Point-to-Point) zur Anwendung. Die nötigen Elemente sind auf das Identifizierungselement 10 und im TTP-Server 40 integriert. Vorzugsweise werden die Transaktionsbelege mit einem symmetrischen Algorithmus verschlüsselt, wobei der symmetrische Algorithmus einen mit einem 25 asymmetrischen Algorithmus verschlüsselten Session Schlüssel benutzt. Vorzugsweise werden ausserdem die übertragenen Transaktionsbelege zertifiziert.

Ansprüche

1. Finanztransaktionsverfahren zwischen einem Kunden und einem Terminal (2), wobei der benannte Kunde mit einem Mobilfunktelefon ausgerüstet ist, das in einem Mobilfunknetz (6) angewendet werden kann, wobei das Mobilfunktelefon ein Mobilgerät (1) und ein wegnehmbares Identifizierungsmodul umfasst, in welchem mindestens eine Kundenidentifizierung und ein elektronischer Geldbetrag gespeichert werden können, wobei das Verfahren mindestens einen von jedem der folgenden 5 Schritte in einer beliebigen Reihenfolge umfasst :
 - Nachladen des benannten Geldbetrages mit Hilfe von Nachladebelegen aus einem Dienstzentrum (4), wobei die benannten Nachladebelege gesichert sind und mittels digitaler Meldungen über das benannte Mobilfunknetz (6) übertragen werden,
- 10 15 - Übertragung der benannten Kundenidentifizierung an das Terminal (2) über eine kontaktlose Schnittstelle zwischen dem benannten Identifizierungsmodul (10) und dem benannten Terminal (2),
 - Prüfung der Erlaubnis des mit der benannten übertragenen Kundenidentifizierung identifizierten Kunden im benannten Terminal, eine 20 Finanztransaktion durchzuführen, wobei diese Prüfung mit Erlaubnisdaten erfolgt, die an das Terminal (2) über ein öffentliches vermitteltes Fernsprechnetz (5) übertragen werden,
 - Übertragung eines elektronischen Transaktionsbetrages über die benannte kontaktlose Schnittstelle an das Terminal (2),
- 25 - Belastung des gespeicherten Geldbetrags in Abhängigkeit des übertragenen Transaktionbetrages,

- Vorbereitung eines Transaktionsbeleges im Terminal (2), welcher die benannte Kundenidentifizierung, eine Terminalidentifizierung sowie eine Angabe über den benannten Transaktionbetrag enthält,
- Elektronische Signierung des benannten Transaktionsbelegs durch 5 das Terminal (2),
- Übertragung des benannten Transaktionsbelegs an das Dienstzentrum (4) über das benannte öffentliche vermittelte Fernsprechnetz (5),
- Prüfung der elektronischen Signatur des Terminals (2) im 10 benannten Dienstzentrum (4),
 - wenn die Signatur einem autorisierten Terminal (2) entspricht, Einzahlung auf einem Konto des Betreibers des Terminals (2).
- 2. Transaktionsverfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass das benannte Dienstzentrum (4) für jeden 15 Kunden ein Kontrollkonto (41) betreibt, in welchem der Wert des im Identifizierungsmodul gespeicherten Geldbetrages gespeichert ist, wobei dieses Kontrollkonto bei jeder Nachladung des benannten Geldbetrages und beim Empfang von Transaktionsbelegen aktualisiert wird.
- 3. Transaktionsverfahren gemäss dem vorhergehenden Anspruch, 20 dadurch gekennzeichnet, dass die benannten Transaktionsbelege an das benannte Dienstzentrum (4) durch eine Clearing-Einheit (3) geleitet werden.
- 4. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Daten, die vom benannten Mobilfunktelefon (1,10) an das Terminal (2) über die benannte kontaktlose 25 Schnittstelle übertragen werden, mit einer elektronischen Signatur des Identifizierungsmoduls (10) versehen sind.

5. Transaktionsverfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannte elektronische Signatur des Identifizierungsmodules (10) im Terminal (2) überprüft wird

6. Transaktionsverfahren gemäss einem der Ansprüche 4 oder 5,
5 dadurch gekennzeichnet, dass die benannte elektronische Signatur des Identifizierungsmodules (10) an das Dienstzentrum (4) weitergeleitet wird und von diesem überprüft wird.

7. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Transaktionsbelege im Batch-
10 Modus über das benannte öffentliche vermittelte Fernsprechnetz (5) an das benannte Dienstzentrum (4) übertragen werden können.

8. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannten Terminals eine Kunden-Schwarzliste enthalten, die vom benannten Dienstzentrum (4) über das
15 benannte öffentliche vermittelte Fernsprechnetz (5) aktualisiert werden kann, und dass die Transaktion unterbrochen wird, wenn die empfangene Kundenidentifizierung in dieser Schwarzliste enthalten ist.

9. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das benannte Dienstzentrum (4) die
20 benannten Identifizierungsmodule (10) mit Hilfe von Kundensperrungsbelegen, die über das benannte Mobilfunknetz (6) übertragen werden, sperren kann.

10. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das benannte Dienstzentrum (4) die benannten Terminals (2) mit Hilfe von Terminalsperrungsbelegen, die über das
25 benannte öffentliche vermittelte Fernsprechnetz (5) übertragen werden, sperren kann.

11. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Identifizierungsmodul (10) eine SIM-Karte ist.

12. Transaktionsverfahren gemäss dem Anspruch 2, dadurch gekennzeichnet, dass das Identifizierungsmodul ein Transponder (10') ist,

und dass das Mobilgerät (24) im Terminal (2) enthalten ist.

13. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Identifizierungsmodul (10, 10') über eine integrierte Spule ins Identifizierungsmodul (10, 10') mit dem Terminal (2) kommuniziert.

14. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Identifizierungsmodul (10) mit Hilfe einer im Mobilgerät (1) integrierten Spule mit dem Terminal (2) kommuniziert.

15. Transaktionsverfahren gemäss einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, dass das Identifizierungsmodul (10) mit Hilfe eines im Mobilgerät (1) integrierten Infrarot-Senders/-Empfängers mit dem Terminal (2) kommuniziert.

16. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens gewisse Daten, die über die benannte kontaktlose Schnittstelle (101-20) zwischen dem Terminal (2) und dem Identifizierungsmodul (10, 10') übertragen, verschlüsselt und/oder signiert werden.

17. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die benannten Transaktionsbelege verschlüsselt werden.

18. Transaktionsverfahren gemäss dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die benannten Transaktionsbelege während der Übertragung nicht entschlüsselt werden.

19. Transaktionsverfahren gemäss einem der Ansprüche 17 oder 18, dadurch gekennzeichnet, dass die Datenelemente (IDUI), die für das Clearing in der benannten Clearing-Einheit (3) benötigt werden, nicht verschlüsselt werden, so dass die Clearing-Einheit die Transaktionsbelege nicht
5 entschlüsseln muss.
20. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Transaktionsbelege (90) mit einem symmetrischen Algorithmus verschlüsselt werden, wobei der symmetrische Algorithmus einen mit einem asymmetrischen Algorithmus
10 verschlüsselten Session Key benutzt.
21. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die durch das bekannte öffentliche ermittelte Netz (5) übertragenen Transaktionsbelege zertifiziert und/oder signiert werden.
15 22. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der benannte Transaktionsbetrag im Terminal (2) gelesen oder erfasst werden kann.
23. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der benannte Transaktionsbetrag im
20 Mobilgerät (1) gelesen oder erfasst werden kann.
24. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Dienstzentrum (4) eine Terminal-Schwarzliste speichert, und dass das Verfahren unterbrochen wird, wenn die empfangene Terminal-Identifizierung (POSID) in der Terminal-Schwarzliste
25 enthalten ist.
25. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Dienstzentrum (4) eine Kundenschwarzliste speichert, und dass das Verfahren unterbrochen wird,

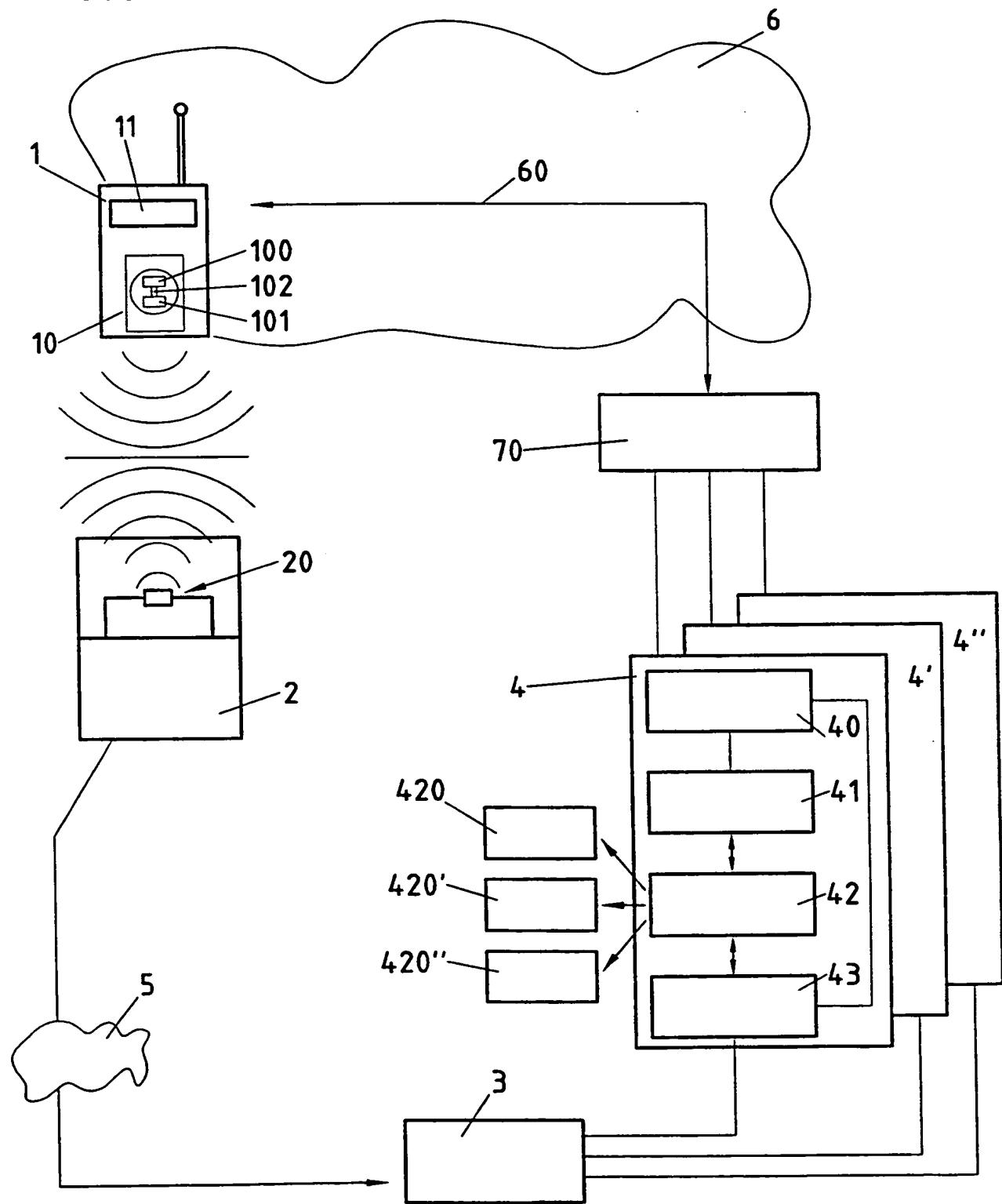
wenn die empfangene Kundenidentifizierung (IDUI) in der Kundenschwarzliste enthalten ist.

26. Transaktionsverfahren gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Identifizierungselement (10) ein
5 Stack mit Daten über bereits durchgeführte Transaktionen enthält,

und dass diese Daten vom Dienstzentrum (4) abgerufen werden können.

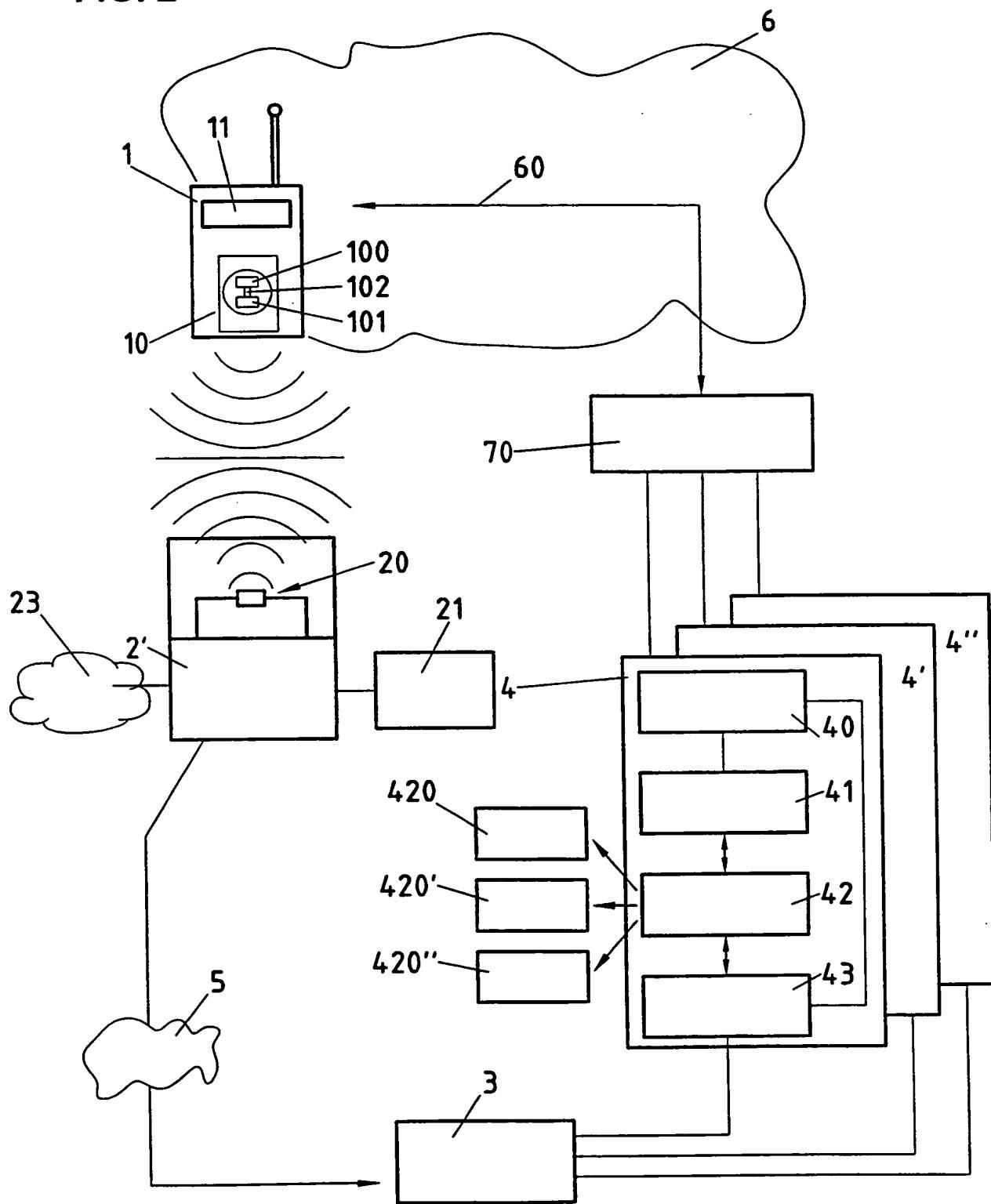
THIS PAGE BLANK (USPTO)

FIG. 1



THIS PAGE BLANK (USPTO)

FIG. 2



THIS PAGE BLANK (USPTO)

3/4

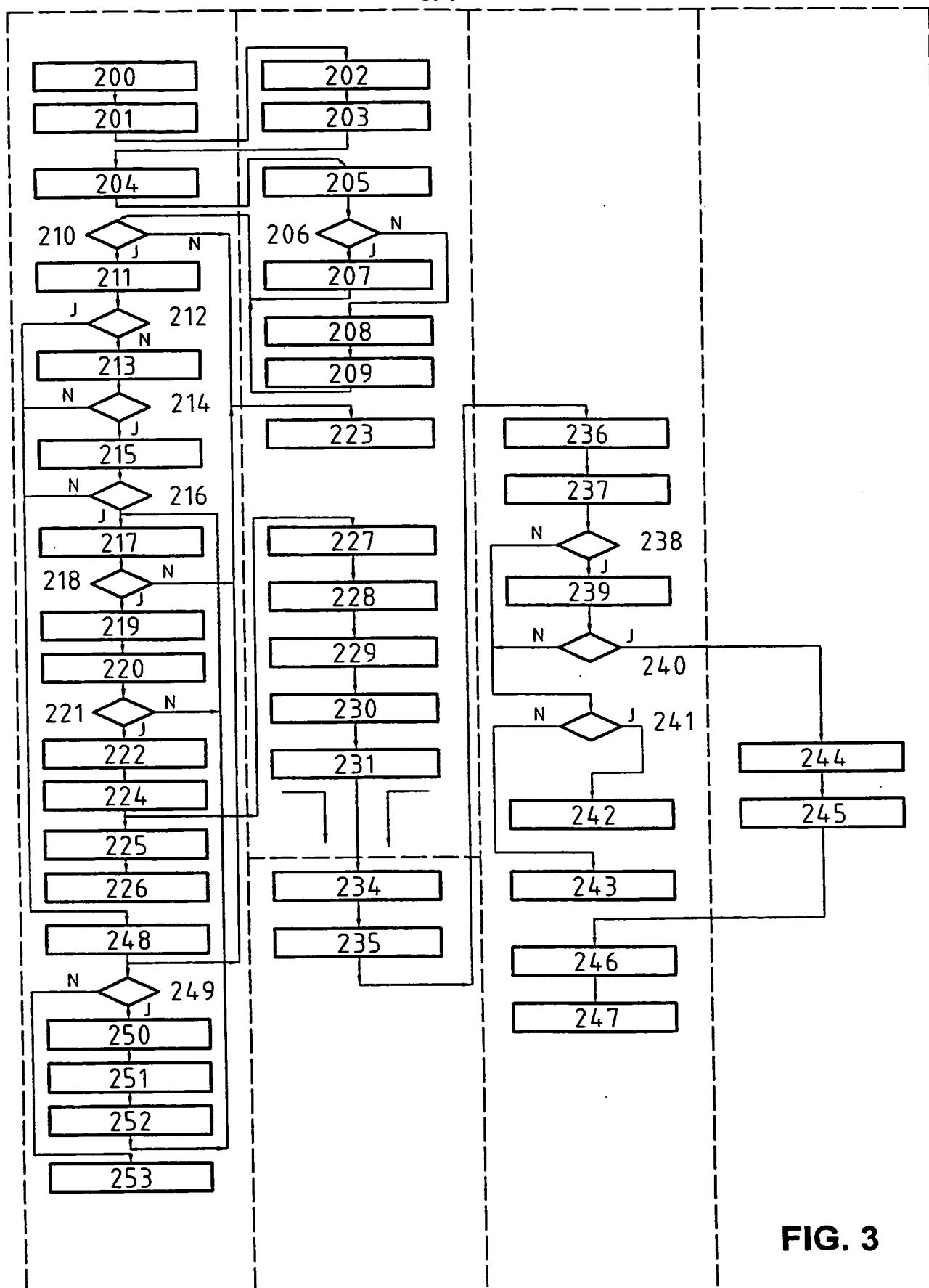


FIG. 3

THIS PAGE BLANK (USPTO)

4/4

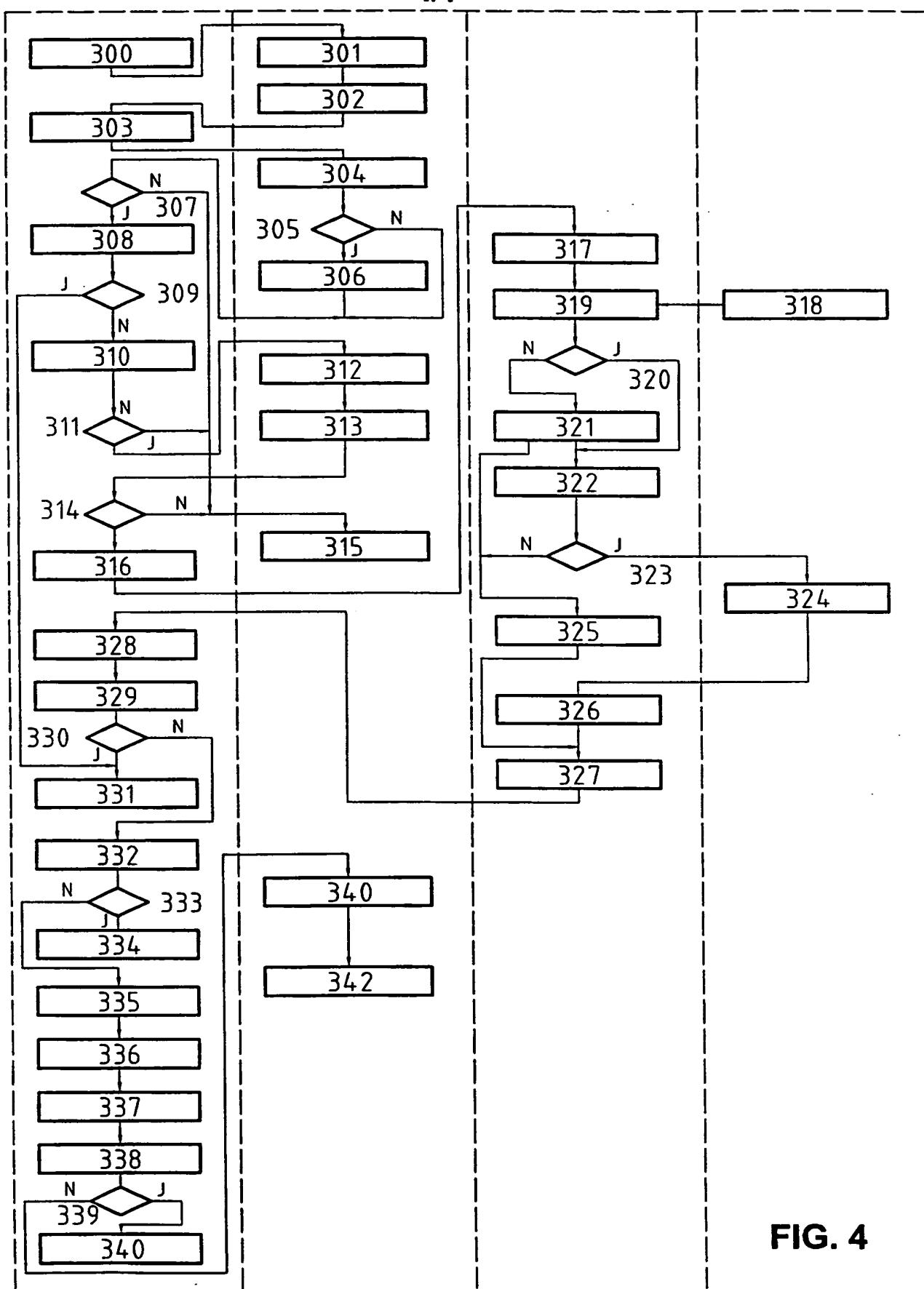


FIG. 4

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

National Application No
PCT/CH 98/00282A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G07F7/08

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	WO 97 45814 A (VAZDAN, B) 4 December 1997	1, 2, 7, 9-11, 21, 23
Y, P	see page 2, line 10 - page 3, line 29 see page 4, line 21 - page 12, line 35; figures 1-9 ---	3
Y	WO 96 18981 A (AKTSIONERNOE OBSCHESTVO ZAKRYT) 20 June 1996 see abstract; figure 1 ---	3
Y A	EP 0 708 547 A (AT&T CORP.) 24 April 1996 see column 2, line 55 - column 8, line 53; figures 1-3 ---	1, 2, 4 3, 5-26
Y	WO 96 13814 A (VAZVAN, B.) 9 May 1996 see page 3, line 7 - page 7, line 24; figures 1-4 ---	1, 2, 4
		-/-

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

31 August 1998

10/09/1998

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Rivero, C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CH 98/00282

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P A	WO 97 46986 A (CKD) 11 December 1997 see page 2, line 18 - page 3, line 6 see page 3, line 15 - page 4, line 29; figures 1,2 ---	1 2,7, 9-11,21, 23
X A	WO 97 14124 A (KONINKLIJKE PTT NEDERLAND N.V.) 17 April 1997 see page 6, line 2 - page 20, line 3; figures 1-5 ---	1 2,4-11, 13-18, 20-26
A	WO 97 18653 A (TRANSACTION TECHNOLOGY, INC.) 22 May 1997 see page 6, line 4 - page 17, line 15; figures 1-4 -----	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/CH 98/00282

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
WO 9745814	A 04-12-1997	FI 962553	A 25-11-1997		
		FI 971248	A 26-04-1997		
		FI 970767	A 20-10-1997		
		FI 971009	A 26-04-1997		
WO 9618981	A 20-06-1996	AU 1904395	A 03-07-1996		
		RU 2096826	C 20-11-1997		
EP 708547	A 24-04-1996	US 5608778	A 04-03-1997		
		CA 2156206	A 23-03-1996		
		JP 8096043	A 12-04-1996		
WO 9613814	A 09-05-1996	FI 945075	A 29-04-1996		
		EP 0739526	A 30-10-1996		
		FI 962553	A 25-11-1997		
		FI 962961	A 28-08-1996		
		FI 971009	A 26-04-1997		
		FI 971248	A 26-04-1997		
		FI 971848	A 30-04-1997		
WO 9746986	A 11-12-1997	FR 2749424	A 05-12-1997		
WO 9714124	A 17-04-1997	NL 1001387	C 11-04-1997		
		AU 2771197	A 19-11-1997		
		AU 5761796	A 18-11-1996		
		AU 7289896	A 30-04-1997		
		WO 9741530	A 06-11-1997		
		EP 0823174	A 11-02-1998		
		NL 1004235	C 11-04-1997		
		NL 1004235	A 11-04-1997		
		NO 974960	A 17-12-1997		
WO 9718653	A 22-05-1997	US 5796832	A 18-08-1998		
		AU 1074597	A 05-06-1997		

THIS PAGE BLANK (USPTO)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/CH 98/00282A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10 G07F7/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X, P	WO 97 45814 A (VAZDAN, B) 4. Dezember 1997	1, 2, 7, 9-11, 21, 23
Y, P	siehe Seite 2, Zeile 10 - Seite 3, Zeile 29 siehe Seite 4, Zeile 21 - Seite 12, Zeile 35; Abbildungen 1-9 ---	3
Y	WO 96 18981 A (AKTSIONERNOE OBSCHESTVO ZAKRYT) 20. Juni 1996 siehe Zusammenfassung; Abbildung 1 ---	3
Y A	EP 0 708 547 A (AT&T CORP.) 24. April 1996 siehe Spalte 2, Zeile 55 - Spalte 8, Zeile 53; Abbildungen 1-3 ---	1, 2, 4 3, 5-26
		-/-

 Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"%" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

Absendedatum des internationalen Recherchenberichts

31. August 1998

10/09/1998

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Rivero, C

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	WO 96 13814 A (VAZVAN, B.) 9. Mai 1996 siehe Seite 3, Zeile 7 - Seite 7, Zeile 24; Abbildungen 1-4 ----	1, 2, 4
X, P	WO 97 46986 A (CKD) 11. Dezember 1997	1
A	siehe Seite 2, Zeile 18 - Seite 3, Zeile 6 siehe Seite 3, Zeile 15 - Seite 4, Zeile 29; Abbildungen 1,2 ----	2, 7, 9-11, 21, 23
X	WO 97 14124 A (KONINKLIJKE PTT NEDERLAND N.V.) 17. April 1997	1
A	siehe Seite 6, Zeile 2 - Seite 20, Zeile 3; Abbildungen 1-5 ----	2, 4-11, 13-18, 20-26
A	WO 97 18653 A (TRANSACTION TECHNOLOGY, INC.) 22. Mai 1997 siehe Seite 6, Zeile 4 - Seite 17, Zeile 15; Abbildungen 1-4 ----	1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

 Internationales Aktenzeichen
PCT/CH 98/00282

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9745814 A	04-12-1997	FI	962553 A	25-11-1997
		FI	971248 A	26-04-1997
		FI	970767 A	20-10-1997
		FI	971009 A	26-04-1997
WO 9618981 A	20-06-1996	AU	1904395 A	03-07-1996
		RU	2096826 C	20-11-1997
EP 708547 A	24-04-1996	US	5608778 A	04-03-1997
		CA	2156206 A	23-03-1996
		JP	8096043 A	12-04-1996
WO 9613814 A	09-05-1996	FI	945075 A	29-04-1996
		EP	0739526 A	30-10-1996
		FI	962553 A	25-11-1997
		FI	962961 A	28-08-1996
		FI	971009 A	26-04-1997
		FI	971248 A	26-04-1997
		FI	971848 A	30-04-1997
WO 9746986 A	11-12-1997	FR	2749424 A	05-12-1997
WO 9714124 A	17-04-1997	NL	1001387 C	11-04-1997
		AU	2771197 A	19-11-1997
		AU	5761796 A	18-11-1996
		AU	7289896 A	30-04-1997
		WO	9741530 A	06-11-1997
		EP	0823174 A	11-02-1998
		NL	1004235 C	11-04-1997
		NL	1004235 A	11-04-1997
		NO	974960 A	17-12-1997
WO 9718653 A	22-05-1997	US	5796832 A	18-08-1998
		AU	1074597 A	05-06-1997

THIS PAGE BLANK (USPTO)

09/446511
416R/PCT/PTO 27 DEC 1999

TRANSLATION

Patent Cooperation Treaty (PCT)

Appointment of an agent or common representative

The undersigned applicant(s) hereby appoint(s)

BOVARD LTD.
Patent Attorneys
Optingenstrasse 16
CH-3000 Berne 25

to act before the competent international authorities concerning the international application filed with the Federal Office of Intellectual Property, 3003 Berne, entitled:

"Transaction Method with a Mobile Device"

Agent's file reference: 81.308/CS/mb

Number of the international application:

Berne

9 June 1998

(Place) Swisscom AG

(Date)

(signature)

(Signature(s) of the Applicant(s))

Swisscom AG
Walter Heutschi

(signature)

(Inventor) Rudolf Ritter

(signature)
(Inventor) Hanspeter Bouquet

(signature)

(Inventor) Walter Heutschi

Please typewrite the name under each signature

THIS PAGE BLANK (USPTO)

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts 81.308/CS/mb	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
Internationales Aktenzeichen PCT/CH98/00282	Internationales Anmeldedatum (Tag/Monat/Jahr) 29/06/1998	Prioritätsdatum (Tag/Monat/Tag) 27/06/1997
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G07F7/10		
Anmelder SWISSCOM AG et al.		
<p>1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.</p> <p>2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.</p> <p><input checked="" type="checkbox"/> Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).</p> <p>Diese Anlagen umfassen insgesamt 3 Blätter.</p>		
<p>3. Dieser Bericht enthält Angaben zu folgenden Punkten:</p> <p>I <input checked="" type="checkbox"/> Grundlage des Berichts II <input type="checkbox"/> Priorität III <input type="checkbox"/> Keine Erstellung eines Gutachtens über Neuheit, erforderliche Tätigkeit und gewerbliche Anwendbarkeit IV <input type="checkbox"/> Mangelnde Einheitlichkeit der Erfindung V <input checked="" type="checkbox"/> Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erforderliche Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung VI <input checked="" type="checkbox"/> Bestimmte angeführte Unterlagen VII <input checked="" type="checkbox"/> Bestimmte Mängel der internationalen Anmeldung VIII <input type="checkbox"/> Bestimmte Bemerkungen zur internationalen Anmeldung</p>		

Datum der Einreichung des Antrags 03/12/1998	Datum der Fertigstellung dieses Berichts 01.07.99
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Bevollmächtigter Bediensteter Rahner, H-G Tel. Nr. (+49-89) 2399 2773



THIS PAGE BLANK (USPTO)

**INTERNATIONALER VORLÄUFIGER
PRÜFUNGSBERICHT**

Internationales Aktenzeichen PCT/CH98/00282

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1,2,4-19	ursprüngliche Fassung
3,3a	eingegangen am 17/04/1999 mit Schreiben vom 13/04/1999

Patentansprüche, Nr.:

1 (Teil),2-26	ursprüngliche Fassung
1 (Teil)	eingegangen am 17/04/1999 mit Schreiben vom 13/04/1999

Zeichnungen, Blätter:

1/4-4/4	ursprüngliche Fassung
---------	-----------------------

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- Beschreibung, Seiten:
- Ansprüche, Nr.:
- Zeichnungen, Blatt:

3. Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

THIS PAGE BLANK (USPTO)

**INTERNATIONALER VORLÄUFIGER
PRÜFUNGSBERICHT**

Internationales Aktenzeichen PCT/CH98/00282

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche 1-26
	Nein: Ansprüche
Erfinderische Tätigkeit (ET)	Ja: Ansprüche 1-26
	Nein: Ansprüche
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche 1-26
	Nein: Ansprüche

2. Unterlagen und Erklärungen

siehe Beiblatt

VI. Bestimmte angeführte Unterlagen

1. Bestimmte veröffentlichte Unterlagen (Regel 70.10)

und / oder

2. Nicht-schriftliche Offenbarungen (Regel 70.9)

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

THIS PAGE BLANK (USPTO)

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erforderlichen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1.) Es wird auf die folgenden Dokumente verwiesen:

D1: WO-A-97 14124
D2: WO-A-97 18653
D3: WO-A-96 13814
D4: WO-A-96 18981

Das Dokument D1 wird als der dem Anmeldungsgegenstand nächstliegende Stand der Technik angesehen. Auch durch D2 (vgl. Zusammenfassung und Seiten 6-17) werden grundlegende Verfahrensabläufe wie Authentifizierung, Verifizierung, Verschlüsselungsmaßnahmen, Kontenführung, Belegerstellung offenbart, wie sie bei dem im vorliegenden Anspruch 1 angegebenen Finanztransaktionen zum Einsatz kommen.

Als weiterer relevanter Stand der Technik im Hinblick auf das anmeldungsgemäße Finanztransaktionsverfahren kommen auch die Druckschriften D3 und D4 in Betracht, nach denen ebenfalls die drahtlose Telekommunikation zur Durchführung finanzieller Transaktionen genutzt wird.

2.) Durch die Druckschrift D1 wird ein Verfahren zur Durchführung finanzieller Transaktionen zwischen einem mit einem Mobilfunktelefon (terminal 8) ausgerüsteten Kunden und einem Terminal (facilitating unit 2 mit support units 3-5) beschrieben, wobei das Mobilfunktelefon ein wegnehmbares Identifizierungsmodul (smart card 9) umfaßt, in welchem eine Kundenidentifizierung und ein elektronischer Geldbetrag gespeichert werden können (vgl. Seite 6, Zeilen 24-26), und wobei der benannte Geldbetrag aus einem Dienstezentrum nachgeladen werden kann (vgl. Seite 4, Zeilen 7-10). Für die Kundenidentifizierung wird ein Übertragungspfad zwischen dem Identifizierungsmodul (smart card 9) und dem Terminal (expansion unit 5) bereitgestellt (vgl. Seite 10, Zeilen 5-8), und zur Prüfung, ob ein Kunde berechtigt ist eine

THIS PAGE BLANK (USPTO)

Transaktion durchzuführen, ist eine terminalseitige Authentifizierungseinheit (transaction unit 3) vorgesehen (vgl. Seite 12, Zeilen 15-19). Der gespeicherte Geldbetrag wird in Abhängigkeit des übertragenen Transaktionsbetrags belastet (vgl. Seite 19, Zeilen 23-25).

- 3). Das Finanztransaktionsverfahren nach dem vorliegenden Anspruch 1 unterscheidet sich vom Stand der Technik gemäß D1 dadurch, daß die Kundenidentifizierung und der Transaktionsbetrag nicht über ein Kommunikationsnetz (wie PSTN- oder GSM-Netzwerk), sondern über eine kontaktlose Schnittstelle zwischen Identifizierungsmodul und Terminal übertragen werden, und daß im Terminal ein Transaktionsbeleg mit der Kundenidentifizierung, einer Terminalidentifizierung, sowie Angaben über den Transaktionsbetrag erstellt und signiert an ein Dienstezentrum übertragen wird. Dadurch können in vorteilhafter Weise eine Vielzahl von Terminals Transaktionen von Kunden gesichert zur zentralisierten Weiterbehandlung an ein Dienstezentrum zur Prüfung der Signatur und der Authentizität des übermittelnden Terminals übertragen.

- 4). Eine Anregung in dieser Hinsicht ist dem verfügbaren relevanten Stand der Technik nicht zu entnehmen. Das im unabhängigen Anspruch 1 definierte Finanztransaktionsverfahren erfüllt daher die Erfordernisse der Neuheit und erfinderschen Tätigkeit gemäß Artikel 33(2) und (3) PCT.
Die gewerbliche Anwendbarkeit des beanspruchten Verfahrens ist offensichtlich gegeben (Artikel 33(4) PCT).

Die Ansprüche 2 bis 26 sind auf den Anspruch 1 rückbezogen und beziehen sich auf besondere Ausgestaltungen des Finanztransaktionsverfahrens. Sie erfüllen daher gleichfalls die Erfordernisse von Artikel 33 PCT.

THIS PAGE BLANK (USPTO)

Zu Punkt VI

Bestimmte angeführte Unterlagen

Bestimmte veröffentlichte Unterlagen (Regel 70.10)

Anmelde Nr. Patent Nr.	Veröffentlichungsdatum (Tag/Monat/Jahr)	Anmelddatum (Tag/Monat/Jahr)	Prioritätsdatum (zu Recht beansprucht) (Tag/Monat/Jahr)
WO-A-9745814	04.12.97	26.05.97	24.05.96; 24.02.97
WO-A-9746986	11.12.97	04.06.97	04.06.96

5). Obwohl die Dokumente WO-A-97 45814 und WO-A-97 46986 keinen Stand der Technik im Sinne der Regel 64.1 b) PCT darstellen, dürften diese Dokumente wesentliche der in der vorliegenden Anmeldung beanspruchten Merkmale offenbaren.
Es wird darauf hingewiesen, daß keine Prüfung der Frage, ob die Priorität gültig ist, durchgeführt worden ist.

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

6). Der Anspruch 1 ist zwar in der zweiteiligen Form abgefaßt; wie vorstehend unter Abschnitt V ausgeführt sind aber unrichtigerweise im kennzeichnenden Teil Merkmale angegeben, die im Dokument D1 in Verbindung mit den im Oberbegriff genannten Merkmalen offenbart wurden (Regel 6.3 b) PCT).

THIS PAGE BLANK (USPTO)

Ausser Debit- und Kreditkarten kennt man die sogenannten e-cash-Karten (Wertkarten), welche es ermöglichen, Geldbeträge elektronisch zu speichern, welche anschliessend an verschiedenen Terminals als Zahlungsmittel akzeptiert werden. Um diese Karten erneut mit Geldbeträgen

5 versehen zu lassen, muss der Kunde am Schalter oder Automaten eines Finanzinstitutes vorstellig werden, was auch nicht immer möglich ist.

Das Patentdokument WO 97/14124 beschreibt ein System, welches das elektronische Bestellen und Bezahlen von Dienstleistungen über ein Kommunikationsnetz, beispielsweise das öffentliche geschaltete Telefonnetz

10 (Public Switched Telephone Network, PSTN) oder ein GSM-Mobilnetz (Global System for Mobile Communication) ermöglicht. Im System gemäss WO 97/14124 kann ein Benutzer mittels einem Kommunikationsendgerät, beispielsweise ein herkömmliches Telefon oder ein Mobilfunktelefon, und mittels Wählimpulsen über ein System mit gesprochener Menuführung Dienste

15 von einer Diensteinheit anfordern. Zur Bezahlung dieser Dienste wird eine „Smart Card“ verwendet, welche über eine Schnittstelle mit dem Kommunikationsendgerät gekoppelt wird und über eine Verbindung dieses Kommunikationsendgeräts mit einer Transaktionseinheit Zahlungsinformationen an diese Transaktionseinheit übermittelt, wobei ein auf

20 der Karte gespeicherter vorausbezahlter Betrag reduziert wird, der gemäss WO 97/14124 auch nachgeladen werden kann. Die „Smart Card“ kann auch nur eine Benutzeridentifizierung umfassen, so dass in der Folge bei einer Bezahlung ein Konto des betreffenden Benutzers belastet wird.

Das Patentdokument WO 97/18653 beschreibt ein System mit

25 mobilen Terminals, über welche ein Benutzer mit einer „Smart Card“, die eine Benutzeridentifizierung und einen Geldbetrag speichert, Finanzinformationen abrufen und Finanztransaktionen ausführen kann, wobei die mobilen Terminal über ein Mobiltelefonnetz mit einem Finanzinstitut verbunden sind.

In der Patentschrift WO 96/13814 wird ein Echtzeitzahlungssystem

30 beschrieben, in welchem Kunden einer Bank mit ihren Mobilfunktelefonen Finanzinformationen abfragen und Rechnungen bezahlen können, indem sie

GEÄNDERTES BLATT

THIS PAGE BLANK (USPTO)

Konto- und Zahlungsinformationen mittels SMS-Meldungen oder über eine Telefonverbindung mit einer Rechnungsstation einer Bank austauschen.

Im Patentdokument WO 96/18981 wird ein Verfahren beschrieben, in welchem biophysikalische Merkmale eines Teilnehmers für dessen

5 Identifizierung bei der Ausführung von Finanz-Clearing-Funktionen verwendet werden.

Eine Aufgabe der vorliegenden Erfindung ist es, ein neues Verfahren oder System vorzuschlagen, das erlaubt, die oben genannten Probleme zu vermeiden.

10 Eine weitere Aufgabe der vorliegenden Erfindung ist es, ein Transaktionsverfahren vorzuschlagen, das sowohl für finanzielle als auch für nicht finanzielle Transaktionen geeignet ist, und das einfacher und zuverlässiger ist, als die gewöhnlichen Transaktionsverfahren.

15 Gemäss der vorliegenden Erfindung werden diese Ziele insbesondere durch die Elemente des kennzeichnenden Teils der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

20 Insbesondere werden diese Ziele durch ein Transaktionsverfahren zwischen einem Kunden und einem mit einem Telekommunikationsnetz verbundenen Terminal (zum Beispiel ein Point-of-Sale, POS) erreicht, welches die Merkmale der unabhängigen Ansprüche umfasst.

Die vorliegende Erfindung wird mit Hilfe der als Beispiel gegebenen Beschreibung besser verständlich und durch die beiliegenden Figuren veranschaulicht :

25 Die Figur 1 zeigt ein Blockschema, das den Informationsfluss in einer ersten Ausführungsform des Systems der Erfindung zeigt, wobei der Kunde mit einem Mobilfunktelefon ausgerüstet ist, vorzugsweise ein GSM- oder UMTS-Mobilgerät, das spezielle Kurzmeldungen empfangen und senden kann.

GEÄNDERTES BLATT

THIS PAGE BLANK (USPTO)

Ansprüche

1. Finanztransaktionsverfahren zwischen einem Kunden und einem Terminal (2), wobei der benannte Kunde mit einem Mobilfunktelefon ausgerüstet ist, das in einem Mobilfunknetz (6) angewendet werden kann, wobei das Mobilfunktelefon ein Mobilgerät (1) und ein wegnehmbares Identifizierungsmodul umfasst, in welchem mindestens eine Kundenidentifizierung und ein elektronischer Geldbetrag gespeichert werden können, wobei der benannte Geldbetrag mit Hilfe von gesicherten Nachladebelegen aus einem Dienstzentrum (4) nachgeladen werden kann, welche Nachladebelege mittels digitaler Meldungen über das benannte Mobilfunknetz (6) übertragen werden, dadurch gekennzeichnet, dass es folgende Schritte umfasst:
 - Übertragung der benannten Kundenidentifizierung an das Terminal (2) über eine kontaktlose Schnittstelle zwischen dem benannten Identifizierungsmodul (10) und dem benannten Terminal (2),
 - Prüfung der Erlaubnis des mit der benannten übertragenen Kundenidentifizierung identifizierten Kunden im benannten Terminal, eine Finanztransaktion durchzuführen, wobei diese Prüfung mit Erlaubnisdaten erfolgt, die an das Terminal (2) über ein öffentliches vermitteltes Fernsprechnetz (5) übertragen werden,
 - Übertragung eines elektronischen Transaktionsbetrages über die benannte kontaktlose Schnittstelle an das Terminal (2),
 - Belastung des gespeicherten Geldbetrags in Abhängigkeit des übertragenen Transaktionbetrages,

GEÄNDERTES BLATT

THIS PAGE BLANK (USPTO)

Even if certain chipcards nowadays contain a microprocessor, these debit cards and credit cards are essentially passive elements which store data that is memorized and used essentially by the electronics of the terminal. The customer, on the other hand, usually has no opportunity of direct access to the data without 5 going to a counter or to an automatic machine of the respective financial institution which issues the card. It is therefore difficult for the customer to check the transactions carried out with the card and to keep a record of them.

These cards contain a customer identification, however, which only allows the customers to be identified at the issuing financial institution. Thus a card can 10 normally only be used for a financial transaction if the customer and the terminal operator are associated with the same financial institution. On the other hand, use of the card for other types of transactions – for example for non-financial transactions for which reliable identification of the customer/ card holder is necessary, however – is not foreseen. Owning a large number of cards for every 15 type of financial and non-financial transactions is therefore unavoidable for the customer, for example several debit cards or credit cards, which are administered by various financial institutions or chains of stores, or subscription cards or access cards for protected zones. These cards are usually protected by various pin codes, which the customer must laboriously memorize.

20 In the case of theft or a fraudulent act using the card, the card must be disabled. The disabling cannot take place, however, until the card has been inserted into a corresponding device. The common credit cards can continue to be used, however, in manually operated apparatuses; a secure blocking of the card is thus not possible.

25 Besides debit cards and credit cards, so-called e-cash cards (value cards) are also known, which enable monetary amounts to be stored electronically, which are then accepted at various terminals as means of payment. To provide these cards again with monetary amounts, the customer must go to the counter or machine of a financial institution, which is not always possible.

THIS PAGE BLANK (USPTO)

The patent document WO 97/14124 describes a system which makes possible the electronic ordering and paying for of services over a telecommunications network, for example the public switched telephone network (Public Switched Telephone Network, PSTN) or a GSM mobile network (Global System for Mobile Communication). In the system according to WO 97/14124 a user can request services from a service unit by means of a communications terminal, for example a conventional telephone or a mobile radio telephone, and by means of dial pulses via a system with spoken menu control. To pay for these services a "smart card" is used, which is coupled to the communications terminal via an interface, and which transmits, via a connection of this communications terminal with a transaction unit, payment information to this transaction unit, a prepaid amount stored on the card being reduced, which according to WO 97/14124 can also be reloaded. The "smart card" can also comprise user identification so that in future during a payment an account of the respective user can be debited.

The patent document WO 97/18653 describes a system with mobile terminals, via which a user with a "smart card," which stores a user identification and a monetary amount, can call up financial information and carry out financial transactions, the mobile terminal being connected to a financial institution via a mobile radio network.

In the patent document WO 96/13814 a real time payment system is described in which customers of a bank can call up financial information and pay bills with their mobile radio telephone in that they exchange account and payment information by means of SMS messages or via a telephone connection with a computing station of a bank.

One object of the present invention is to propose a method or system which allows these problems to be avoided.

THIS PAGE BLANK (USPTO)

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts 81.308/CS/mb	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/CH 98/ 00282	Internationales Anmeldedatum (Tag/Monat/Jahr) 29/06/1998	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 27/06/1997
Anmelder SWISSCOM AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 4 Blätter.

Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen (siehe Feld I).
2. Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).
3. In der internationalen Anmeldung ist ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt.
 - das zusammen mit der internationalen Anmeldung eingereicht wurde.
 - das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde,
 - dem jedoch keine Erklärung beigelegt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
 - das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.
4. Hinsichtlich der Bezeichnung der Erfindung
 - wird der vom Anmelder eingereichte Wortlaut genehmigt.
 - wurde der Wortlaut von der Behörde wie folgt festgesetzt.
5. Hinsichtlich der Zusammenfassung
 - wird der vom Anmelder eingereichte Wortlaut genehmigt.
 - wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.
6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen:
Abb. Nr. 1 wie vom Anmelder vorgeschlagen keine der Abb.
 - weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
 - weil diese Abbildung die Erfindung besser kennzeichnet.

THIS PAGE BLANK (USPTO)

INTERNATIONALER RECHERCHENBERICHT

internationales Aktenzeichen

PCT/CH 98/ 00282

F Id III WORTLAUT DER ZUSAMMENFASSUNG (Fortsetzung von Punkt 5 auf Blatt 1)

Die Zusammenfassung wird wie folgt geändert:

Zeile 6: nach "Verfahren" ist "einem von jedem der" einzufügen;

Zeile 6: "folgende" werden "folgenden"

Zeile 19:

Der mit den Worten "-Balastung" beginnende und den Worten "Terminals." (Zeile 30) endende Teil ist zu streichen.

THIS PAGE BLANK (USPTO)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/CH 98/00282A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10 G07F7/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X, P	WO 97 45814 A (VAZDAN, B) 4. Dezember 1997	1, 2, 7, 9-11, 21, 23
Y, P	siehe Seite 2, Zeile 10 - Seite 3, Zeile 29 siehe Seite 4, Zeile 21 - Seite 12, Zeile 35; Abbildungen 1-9 ---	3
Y	WO 96 18981 A (AKTSIONERNOE OBSCHESTVO ZAKRYT) 20. Juni 1996 siehe Zusammenfassung; Abbildung 1 ---	3
Y A	EP 0 708 547 A (AT&T CORP.) 24. April 1996 siehe Spalte 2, Zeile 55 - Spalte 8, Zeile 53; Abbildungen 1-3 ---	1, 2, 4 3, 5-26
		-/-

 Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"g" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

Absendedatum des internationalen Recherchenberichts

31. August 1998

10/09/1998

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Rivero, C

THIS PAGE BLANK (USPTO)

INTERNATIONALER FISCHERCHENBERICHT

Internationales Aktenzeichen

PCT/CH 98/00282

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	WO 96 13814 A (VAZVAN, B.) 9. Mai 1996 siehe Seite 3, Zeile 7 - Seite 7, Zeile 24; Abbildungen 1-4 ---	1,2,4
X, P	WO 97 46986 A (CKD) 11. Dezember 1997 siehe Seite 2, Zeile 18 - Seite 3, Zeile 6	1
A	siehe Seite 3, Zeile 15 - Seite 4, Zeile 29; Abbildungen 1,2 ---	2,7, 9-11,21, 23
X	WO 97 14124 A (KONINKLIJKE PTT NEDERLAND N.V.) 17. April 1997	1
A	siehe Seite 6, Zeile 2 - Seite 20, Zeile 3; Abbildungen 1-5 ---	2,4-11, 13-18, 20-26
A	WO 97 18653 A (TRANSACTION TECHNOLOGY, INC.) 22. Mai 1997 siehe Seite 6, Zeile 4 - Seite 17, Zeile 15; Abbildungen 1-4 -----	1

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/CH 98/00282

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9745814	A	04-12-1997	FI	962553 A	25-11-1997
			FI	971248 A	26-04-1997
			FI	970767 A	20-10-1997
			FI	971009 A	26-04-1997
WO 9618981	A	20-06-1996	AU	1904395 A	03-07-1996
			RU	2096826 C	20-11-1997
EP 708547	A	24-04-1996	US	5608778 A	04-03-1997
			CA	2156206 A	23-03-1996
			JP	8096043 A	12-04-1996
WO 9613814	A	09-05-1996	FI	945075 A	29-04-1996
			EP	0739526 A	30-10-1996
			FI	962553 A	25-11-1997
			FI	962961 A	28-08-1996
			FI	971009 A	26-04-1997
			FI	971248 A	26-04-1997
			FI	971848 A	30-04-1997
WO 9746986	A	11-12-1997	FR	2749424 A	05-12-1997
WO 9714124	A	17-04-1997	NL	1001387 C	11-04-1997
			AU	2771197 A	19-11-1997
			AU	5761796 A	18-11-1996
			AU	7289896 A	30-04-1997
			WO	9741530 A	06-11-1997
			EP	0823174 A	11-02-1998
			NL	1004235 C	11-04-1997
			NL	1004235 A	11-04-1997
			NO	974960 A	17-12-1997
WO 9718653	A	22-05-1997	US	5796832 A	18-08-1998
			AU	1074597 A	05-06-1997

THIS PAGE BLANK (USPTO)

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

PTO/PCT REC'D For receiving Office use only
DEC 1999

International Application No.

International Filing Date

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference 81.308/CS/mb
(if desired) (12 characters maximum)

Box No. I TITLE OF INVENTION

Transaction Method with a Mobile Device

Box No. II APPLICANT

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

SWISSCOM
Viktoriastrasse 21
3050 Berne (Switzerland)

This person is also inventor.

Telephone No.

Faximile No.

Teleprinter No.

State (that is, country) of nationality:
Switzerland

State (that is, country) of residence:
Switzerland

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

RITTER, Rudolf
Rossweidweg 8
3052 Zollikofen (Switzerland)

This person is:

applicant only

applicant and inventor

inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:
Switzerland

State (that is, country) of residence:
Switzerland

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:

agent

common representative

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

BOVARD LTD.
Patent Attorneys
Optingenstrasse 16
3000 Berne 25 (Switzerland)

Telephone No.

031/335 20 00

Faximile No.

031/332 81 59

Teleprinter No.

911 907 bova ch

Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

THIS PAGE BLANK (USPTO)

Continuation of Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

BOUQUET, Hanspeter
Kappelenring 49A
3032 Hinterkappelen (Switzerland)

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

Switzerland

State (that is, country) of residence:

Switzerland

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

HEUTSCHI, Walter
Jungfrauweg 8
3303 Jegenstorf (Switzerland)

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

Switzerland

State (that is, country) of residence:

Switzerland

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

State (that is, country) of residence:

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

This person is:

applicant only
 applicant and inventor
 inventor only (If this check-box is marked, do not fill in below.)

State (that is, country) of nationality:

State (that is, country) of residence:

This person is applicant for the purposes of: all designated States all designated States except the United States of America the United States of America only the States indicated in the Supplemental Box

Further applicants and/or (further) inventors are indicated on another continuation sheet.

THIS PAGE BLANK (USPTO)

Box No. V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) (mark the applicable check-boxes; at least one must be marked):

Regional Patent

AP ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SL Sierra Leone, SZ Swaziland, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT

EA Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

EP European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

OA OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)

National Patent (if other kind of protection or treatment desired, specify on dotted line):

AL Albania

AM Armenia

AT Austria

AU Australia

AZ Azerbaijan

BA Bosnia and Herzegovina

BB Barbados

BG Bulgaria

BR Brazil

BY Belarus

CA Canada

CH and LI Switzerland and Liechtenstein

CN China

CU Cuba

CZ Czech Republic

DE Germany

DK Denmark

EE Estonia

ES Spain

FI Finland

GB United Kingdom

GE Georgia

GH Ghana

GM Gambia

GW Guinea-Bissau

HU Hungary

ID Indonesia

IL Israel

IS Iceland

JP Japan

KE Kenya

KG Kyrgyzstan

KP Democratic People's Republic of Korea

KR Republic of Korea

KZ Kazakhstan

LC Saint Lucia

LK Sri Lanka

LR Liberia

LS Lesotho

LT Lithuania

LU Luxembourg

LV Latvia

MD Republic of Moldova

MG Madagascar

MK The former Yugoslav Republic of Macedonia

MN Mongolia

MW Malawi

MX Mexico

NO Norway

NZ New Zealand

PL Poland

PT Portugal

RO Romania

RU Russian Federation

SD Sudan

SE Sweden

SG Singapore

SI Slovenia

SK Slovakia

SL Sierra Leone

TJ Tajikistan

TM Turkmenistan

TR Turkey

TT Trinidad and Tobago

UA Ukraine

UG Uganda

US United States of America

UZ Uzbekistan

VN Viet Nam

YU Yugoslavia

ZW Zimbabwe

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

.....

.....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)

THIS PAGE BLANK (USPTO)

Box No. VI PRIORITY CLAIM		Further priority claims are indicated in the Supplemental Box <input type="checkbox"/>																					
The priority of the following earlier application(s) is hereby claimed:																							
Country (in which, or for which, the application was filed)	Filing Date (day/month/year)	Application No.	Office of filing (only for regional or international application)																				
item (1) Switzerland	27.06.1997 (27 June 1997)	1564/97																					
item (2) PCT (Switzerland) (5 March 1998)	05.03.1998	PCT/CH 98/00086																					
item (3)																							
<p>Mark the following check-box if the certified copy of the earlier application is to be issued by the Office which for the purposes of the present international application is the receiving Office (a fee may be required):</p> <p><input type="checkbox"/> The receiving Office is hereby requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s) : _____</p>																							
Box No. VII INTERNATIONAL SEARCHING AUTHORITY																							
<p>Choice of International Searching Authority (ISA) (If two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used): ISA / _____</p> <p>Earlier search Fill in where a search (international, international-type or other) by the International Searching Authority has already been carried out or requested and the Authority is now requested to base the international search, to the extent possible, on the results of that earlier search. Identify such search or request either by reference to the relevant application (or the translation thereof) or by reference to the search request.</p>																							
Country (or regional Office):	Date (day/month/year):	Number:																					
European Patent Office	26 June 1998	PCT/CH 98/00086																					
Box No. VIII CHECK LIST																							
<p>This international application contains the following number of sheets:</p> <table> <tr> <td>1. request</td> <td>: 4 sheets</td> </tr> <tr> <td>2. description</td> <td>: 19 sheets</td> </tr> <tr> <td>3. claims</td> <td>: 6 sheets</td> </tr> <tr> <td>4. abstract</td> <td>: 2 sheets</td> </tr> <tr> <td>5. drawings</td> <td>: 4 sheets</td> </tr> <tr> <td>Total</td> <td>: 35 sheets</td> </tr> </table>	1. request	: 4 sheets	2. description	: 19 sheets	3. claims	: 6 sheets	4. abstract	: 2 sheets	5. drawings	: 4 sheets	Total	: 35 sheets	<p>This international application is accompanied by the item(s) marked below:</p> <table> <tr> <td>1. <input checked="" type="checkbox"/> separate signed power of attorney</td> <td>5. <input type="checkbox"/> fee calculation sheet follows</td> </tr> <tr> <td>2. <input type="checkbox"/> copy of general power of attorney</td> <td>6. <input type="checkbox"/> separate indications concerning deposited microorganisms</td> </tr> <tr> <td>3. <input type="checkbox"/> statement explaining lack of signature</td> <td>7. <input type="checkbox"/> nucleotide and/or amino acid sequence listing (diskette)</td> </tr> <tr> <td>4. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s): follows</td> <td>8. <input checked="" type="checkbox"/> other (specify): Copy Search Report</td> </tr> </table>			1. <input checked="" type="checkbox"/> separate signed power of attorney	5. <input type="checkbox"/> fee calculation sheet follows	2. <input type="checkbox"/> copy of general power of attorney	6. <input type="checkbox"/> separate indications concerning deposited microorganisms	3. <input type="checkbox"/> statement explaining lack of signature	7. <input type="checkbox"/> nucleotide and/or amino acid sequence listing (diskette)	4. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s): follows	8. <input checked="" type="checkbox"/> other (specify): Copy Search Report
1. request	: 4 sheets																						
2. description	: 19 sheets																						
3. claims	: 6 sheets																						
4. abstract	: 2 sheets																						
5. drawings	: 4 sheets																						
Total	: 35 sheets																						
1. <input checked="" type="checkbox"/> separate signed power of attorney	5. <input type="checkbox"/> fee calculation sheet follows																						
2. <input type="checkbox"/> copy of general power of attorney	6. <input type="checkbox"/> separate indications concerning deposited microorganisms																						
3. <input type="checkbox"/> statement explaining lack of signature	7. <input type="checkbox"/> nucleotide and/or amino acid sequence listing (diskette)																						
4. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s): follows	8. <input checked="" type="checkbox"/> other (specify): Copy Search Report																						
<p>Figure No. 1 of the drawings (if any) should accompany the abstract when it is published.</p>																							
Box No. IX SIGNATURE OF APPLICANT OR AGENT																							
<p>Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).</p>																							
<p>BOVARD LTD.</p> <p>J. Aebischer</p>																							

For receiving Office use only		
<p>1. Date of actual receipt of the purported international application:</p> <p>3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:</p> <p>4. Date of timely receipt of the required corrections under PCT Article 11(2):</p> <p>5. International Searching Authority ISA /</p>		<p>2. Drawings:</p> <p><input type="checkbox"/> received:</p> <p><input type="checkbox"/> not received:</p>
<p>6. <input type="checkbox"/> Transmittal of search copy delayed until search fee is paid</p>		

For International Bureau use only	
<p>Date of receipt of the record copy by the International Bureau:</p>	

THIS PAGE BLANK (USPTO)

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICH NACH DEM VERTRAG ÜBER DIE
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G07F 7/10, 7/08	A1	(11) Internationale Veröffentlichungsnummer: WO 99/00773 (43) Internationales Veröffentlichungsdatum: 7. Januar 1999 (07.01.99)
(21) Internationales Aktenzeichen: PCT/CH98/00282		(81) Bestimmungsstaaten: AL, AM, AT, AT (Gebrauchsmuster), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Gebrauchsmuster), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).
(22) Internationales Anmeldedatum: 29. Juni 1998 (29.06.98)		
(30) Prioritätsdaten: 1564/97 27. Juni 1997 (27.06.97) CH PCT/CH98/00086 5. März 1998 (05.03.98) WO (34) Länder für die die regionale oder internationale Anmeldung eingereicht worden ist: CH usw.		
(71) Anmelder (für alle Bestimmungsstaaten ausser US): SWISS- COM AG [CH/CH]; Viktoriastrasse 21, CH-3050 Bern (CH).		Veröffentlicht Mit internationalem Recherchenbericht.
(72) Erfinder; und		
(75) Erfinder/Anmelder (nur für US): RITTER, Rudolf [CH/CH]; Rossweidweg 8, CH-3052 Zollikofen (CH). BOUQUET, Hanspeter [CH/CH]; Kappelenring 49A, CH-3032 Hinterkappelen (CH). HEUTSCHI, Walter [CH/CH]; Jungfrauweg 8, CH-3303 Jegenstorf (CH).		
(74) Anwalt: BOVARD AG; Optingenstrasse 16, CH-3000 Bern 25 (CH).		

(54) Title: TRANSACTION METHOD CARRIED OUT WITH A MOBILE APPARATUS

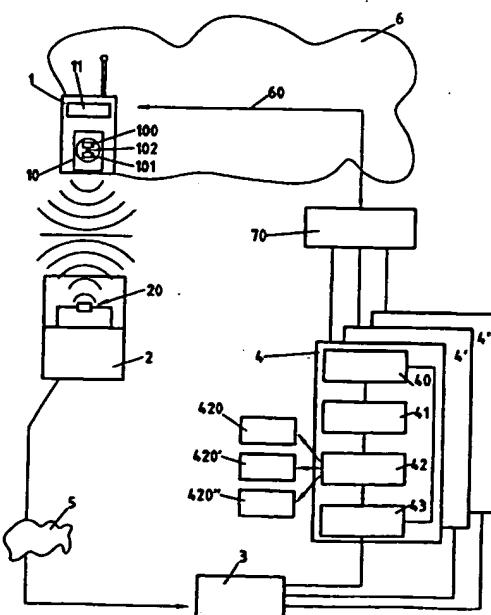
(54) Bezeichnung: TRANSAKTIONSVERFAHREN MIT EINEM MOBILGERÄT

(57) Abstract

The invention relates to a method for carrying out financial transactions between a client equipped with a mobile telephone and an electronic terminal (2), where said mobile telephone comprises a mobile apparatus (1) and a detachable identification module in which at least one client identification element and one electronic sum of money can be memorized. Said method comprises each of the following steps: reloading of the given sum of money by means of secured reloading documents via the mobile telephone network from a service centre (4), transmission of the client identification element to the terminal (2) via a contactless interface between the identification module (10) and the terminal (2), verification in said terminal that the client identified by means of the aforementioned transmitted client identification element is authorized to carry out a financial transaction, said verification being carried out with authorization data transmitted to the terminal (2) via a public connected telephone network (5), and transmission of a transaction amount to the terminal (2) via the contactless interface.

(57) Zusammenfassung

Finanztransaktionsverfahren zwischen einem mit einem Mobilfunktelefon ausgerüsteten Kunden und einem elektronischen Terminal (2), wobei das Mobilfunktelefon ein Mobilgerät (1) und ein wegznehmbares Identifizierungsmodul umfasst, in welchem mindestens eine Kundenidentifizierung und ein elektronischer Geldbetrag gespeichert werden können, wobei das Verfahren einen von jedem der folgenden Schritte umfasst: Nachladen des benannten Geldbetrages mit Hilfe von gesicherten Nachladebögen über das Mobilfunknetz aus einem Dienstzentrum (4); Übertragung der Kundenidentifizierung an das Terminal (2) über eine kontaktlose Schnittstelle zwischen dem Identifizierungsmodul (10) und dem Terminal (2); Prüfung im benannten Terminal der Erlaubnis des mit der benannten übertragenen Kundenidentifizierung identifizierten Kunden, eine Finanztransaktion durchzuführen, wobei diese Prüfung mit Erlaubnisdaten erfolgt, die an das Terminal (2) über ein öffentliches vermitteltes Fernsprechnetz (5) übertragen werden; Übertragung eines Transaktionsbetrages über die kontaktlose Schnittstelle an das Terminal (2).



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Application No

PCT/CH 98/00282

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 G07F7/10 G07F7/08

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	WO 97 45814 A (VAZDAN, B) 4 December 1997	1, 2, 7, 9-11, 21, 23
Y, P	see page 2, line 10 - page 3, line 29 see page 4, line 21 - page 12, line 35; figures 1-9 ---	3
Y	WO 96 18981 A (AKTSIONERNOE OBSCHESTVO ZAKRYT) 20 June 1996 see abstract; figure 1 ---	3
Y A	EP 0 708 547 A (AT&T CORP.) 24 April 1996 see column 2, line 55 - column 8, line 53; figures 1-3 ---	1, 2, 4 3, 5-26
Y	WO 96 13814 A (VAZVAN, B.) 9 May 1996 see page 3, line 7 - page 7, line 24; figures 1-4 ---	1, 2, 4
		-/-

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

31 August 1998

10/09/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patenttaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

Rivero, C

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Application No
PCT/CH 98/00282

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P A	WO 97 46986 A (CKD) 11 December 1997 see page 2, line 18 - page 3, line 6 see page 3, line 15 - page 4, line 29; figures 1,2 ---	1 2,7, 9-11,21, 23
X A	WO 97 14124 A (KONINKLIJKE PTT NEDERLAND N.V.) 17 April 1997 see page 6, line 2 - page 20, line 3; figures 1-5 ---	1 2,4-11, 13-18, 20-26
A	WO 97 18653 A (TRANSACTION TECHNOLOGY, INC.) 22 May 1997 see page 6, line 4 - page 17, line 15; figures 1-4 -----	1

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Information for patent family members

Application No

PCT/CH 98/00282

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 9745814	A 04-12-1997	FI FI FI FI	962553 A 971248 A 970767 A 971009 A	25-11-1997 26-04-1997 20-10-1997 26-04-1997
WO 9618981	A 20-06-1996	AU RU	1904395 A 2096826 C	03-07-1996 20-11-1997
EP 708547	A 24-04-1996	US CA JP	5608778 A 2156206 A 8096043 A	04-03-1997 23-03-1996 12-04-1996
WO 9613814	A 09-05-1996	FI EP FI FI FI FI FI	945075 A 0739526 A 962553 A 962961 A 971009 A 971248 A 971848 A	29-04-1996 30-10-1996 25-11-1997 28-08-1996 26-04-1997 26-04-1997 30-04-1997
WO 9746986	A 11-12-1997	FR	2749424 A	05-12-1997
WO 9714124	A 17-04-1997	NL AU AU AU WO EP NL NL NO	1001387 C 2771197 A 5761796 A 7289896 A 9741530 A 0823174 A 1004235 C 1004235 A 974960 A	11-04-1997 19-11-1997 18-11-1996 30-04-1997 06-11-1997 11-02-1998 11-04-1997 11-04-1997 17-12-1997
WO 9718653	A 22-05-1997	US AU	5796832 A 1074597 A	18-08-1998 05-06-1997

THIS PAGE BLANK (USPTO)